

# Cours d'algèbre de licence à l'université de NICE en 1978-79

donnés par Jean-Michel LEMAIRE
recopié par Dany-Jack MERCIER

COURS et TD
d'ALGEBRE
(LICENCE)

Cours d'algèbre de licence à l'université de NICE en 1978-79
donnés par Jean-Michel LEMAIRE et recopié par Dany-Jack MERCIER.

# 1 Généralités sur les groupes

**Def** | groupe monogène fini $\Leftrightarrow$ groupe cyclique.

**Th** | Tout groupe monogène est
1) isomorphe à $\mathbb{Z}$ s'il est infini
2) isomorphe à $\mathbb{Z}/n\mathbb{Z}$ s'il est fini d'ordre n

Remarques (plutôt) : Inversement, tout groupe isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$ est monogène.

**Th** | $G$ = groupe monogène d'ordre n $\Leftrightarrow$ $G$ isomorphe à $\mathbb{Z}/n\mathbb{Z}$

($\Leftarrow$) Il existe $\varphi$ isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur $G$

$$\varphi : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$$
$$\dot{0} \longmapsto e$$
$$\dot{1} \longmapsto a \quad (a \neq e)$$
$$\cdots$$

par récurrence : $\dot{x} \longmapsto \varphi(\dot{x}) = a^x \quad (\forall x \in \mathbb{Z})$

Et donc $\dot{n} = \dot{0} \Rightarrow \varphi(\dot{n}) = \varphi(\dot{0}) \Rightarrow a^n = e$

Ainsi : $\operatorname{Im}\varphi = \{e, a, \ldots, a^{n-1}\}$

$G$ est bien un groupe monogène (d'ordre n)

($\Rightarrow$) Soit $G = \{e, a, \ldots, a^{n-1}\}$ un groupe monogène ($G = \langle a \rangle$)

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\psi} & G \\ \pi \downarrow & & \uparrow \\ \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\varphi \text{ iso.}} & \psi(\mathbb{Z}) = G \end{array} \qquad \psi(p) = a^p$$

($n\mathbb{Z} = \ker\psi$ puisque $a^n = e$)

**Th** | $G$ = groupe d'ordre p <u>premier</u> $\Rightarrow$ $G$ isomorphe à $\mathbb{Z}/p\mathbb{Z}$

(cf. polycop. p. (I)2)

**Conséquence :**

$G$ = groupe d'ordre $p$ premier $\Rightarrow$ $G$ monogène d'ordre $p$.
$(\exists a \in G \setminus \{e\} \;/\; G = \{e, a, \dots, a^{p-1}\})$

Etude de $\mathfrak{S}_3$

**Liste des groupes finis**

| nbre élt. | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| | $\{e\}$ | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Z}/4\mathbb{Z}$ | $\mathbb{Z}/5\mathbb{Z}$ | $\mathbb{Z}/6\mathbb{Z}$ | $\mathbb{Z}/7\mathbb{Z}$ | $\mathbb{Z}/8\mathbb{Z}$ |
| | | | | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ KLEIN | | $\mathfrak{S}_3$ (non com.) | | $(\mathbb{Z}/2\mathbb{Z})^3$ |
| | | | | | | | | $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ |
| | | | | | | | | $H$ |
| | | | | | | | | $D_4$ |

non abéliens ($\mathfrak{S}_3$, $H$)

**Sous-groupes de $\mathfrak{S}_3$**

$G$ s.groupe de $\mathfrak{S}_3 \Rightarrow$ ordre$(G)$ divise ordre$(\mathfrak{S}_3) = 6$

Pour $G \neq \{Id\} \cup \mathfrak{S}_3$, deux cas possibles :

$*$ ord$(G) = 3$ premier $\Rightarrow G$ iso. à $\mathbb{Z}/3\mathbb{Z} \Rightarrow G$ monogène

$G = \{1, (3,2,1), (3,1,2)\} = \mathfrak{A}_3$

(cycles)

* ordre $(G) = 2$ premier $\Rightarrow$ $G \simeq \mathbb{Z}/2\mathbb{Z}$ $\Rightarrow$ $G$ monogène

3 groupes :

$\{1, (1,2)\}$

$\{1, (2,3)\}$

$\{1, (1,3)\}$

Remarque : $< (1,2) ; (2,3) > = \mathcal{S}_3$

$a_3$ est forcément un sous-groupe distingué : Sinon, il ne serait pas invariant par tout automorphisme intérieur, et il existerait un autre sous-groupe d'ordre 3, ce qui n'est pas.

Une autre raison pour s'apercevoir que $a_3$ est distingué est :

On considère sign ("signature") $\mathcal{S}_3 \longrightarrow \{-1, 1\}$

$$\sigma \longmapsto \text{sign}(\sigma) = \frac{\prod_{\substack{i>j \\ i=1,\dots,n \\ j=1,\dots,n}} (\sigma(i)-\sigma(j))}{\prod (i-j)}$$

Alors sign définit un homomorphisme de groupe qui vaut $(-1)$ sur les transpositions.

$a_3 = \{\sigma \ / \ \text{sign}(\sigma) = 1\} = \text{Ker sign}$

c'est donc bien un s-groupe distingué de $\mathcal{S}_3$

<u>Décomposition d'une permutation en cycles disjoints</u>

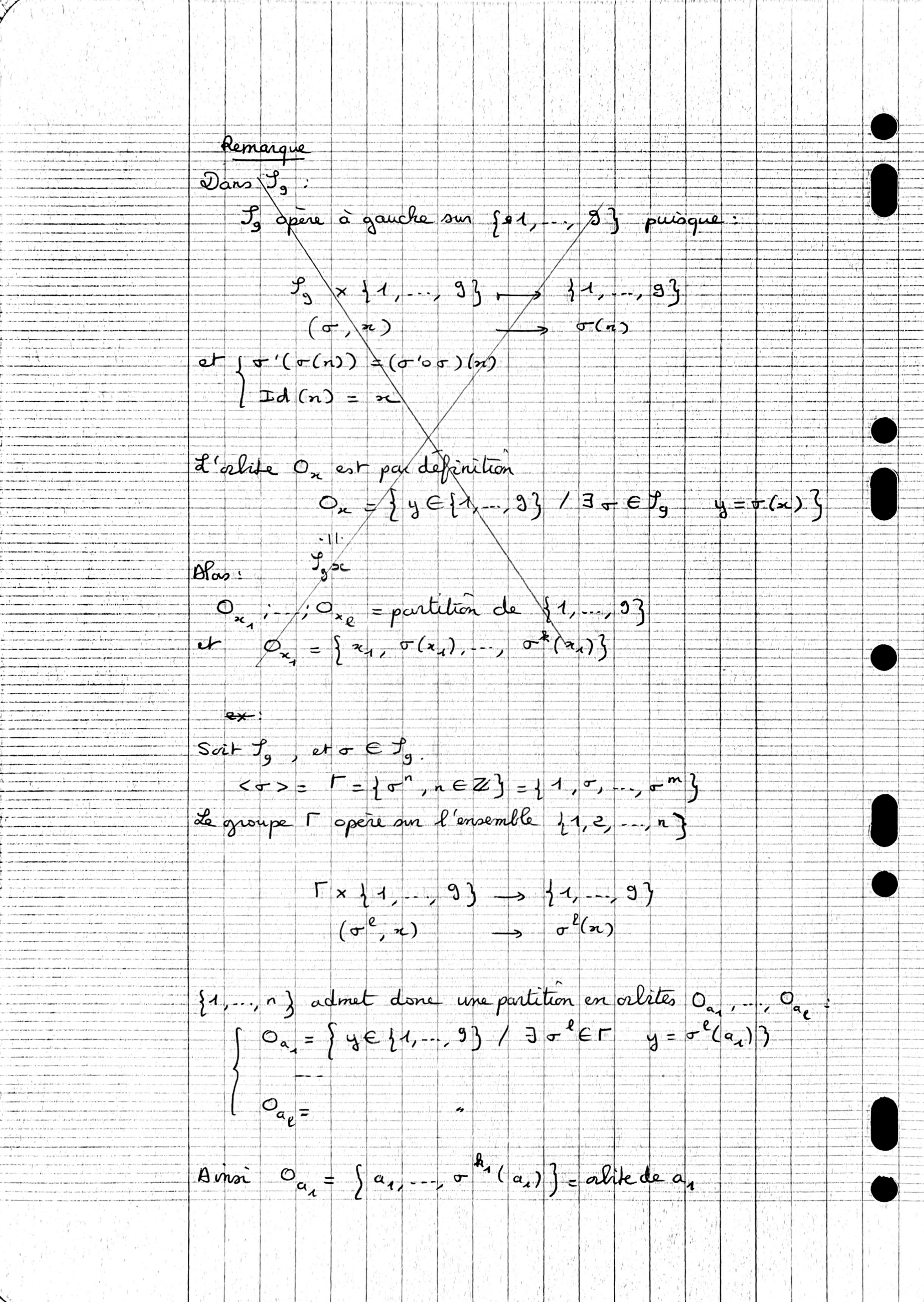
ex :

$$\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 7 & 5 & 1 & 2 & 8 & 9 & 6 \end{pmatrix}$$

$(1 \ 4 \ 5)$ ↳ retour en 1 : $\gamma_1$ = cycle

$(2, 3, 7, 8, 9, 6)$ ↳ retour en 2 : $\gamma_2$ = cycle

On a $\sigma = \gamma_2 \circ \gamma_1 = \gamma_1 \circ \gamma_2$



<u>Remarque</u>

Dans $S_9$ :

$S_9$ opère à gauche sur $\{1, \dots, 9\}$ puisque :

$$S_9 \times \{1, \dots, 9\} \longrightarrow \{1, \dots, 9\}$$
$$(\sigma, x) \longrightarrow \sigma(x)$$

et $\begin{cases} \sigma'(\sigma(x)) = (\sigma' \circ \sigma)(x) \\ Id(x) = x \end{cases}$

L'orbite $O_x$ est par définition

$$O_x = \{ y \in \{1, \dots, 9\} \ / \ \exists \sigma \in S_9 \quad y = \sigma(x) \}$$
$$= S_9 x$$

Alors :

$O_{x_1}; \dots ; O_{x_\ell}$ = partition de $\{1, \dots, 9\}$

et $O_{x_1} = \{ x_1, \sigma(x_1), \dots, \sigma^k(x_1) \}$

~~ex~~ :

Soit $S_9$, et $\sigma \in S_9$.

$$\langle \sigma \rangle = \Gamma = \{ \sigma^n, n \in \mathbb{Z} \} = \{ 1, \sigma, \dots, \sigma^m \}$$

Le groupe $\Gamma$ opère sur l'ensemble $\{1, 2, \dots, n\}$

$$\Gamma \times \{1, \dots, 9\} \longrightarrow \{1, \dots, 9\}$$
$$(\sigma^\ell, x) \longrightarrow \sigma^\ell(x)$$

$\{1, \dots, n\}$ admet donc une partition en orbites $O_{a_1}, \dots, O_{a_\ell}$ :

$$\begin{cases} O_{a_1} = \{ y \in \{1, \dots, 9\} \ / \ \exists \sigma^\ell \in \Gamma \quad y = \sigma^\ell(a_1) \} \\ \dots \\ O_{a_\ell} = \quad " \end{cases}$$

Ainsi $O_{a_1} = \{ a_1, \dots, \sigma^{k_1}(a_1) \}$ = orbite de $a_1$

Pour $\sigma$ de l'exemple précédent :

$O_1 = \{1, 4, 5\}$ = orbite de 1 sous $\Gamma = \langle \sigma \rangle$

$O_2 = \{2, 3, 7, 8, 9, 6\}$

$$1 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 1 \qquad 2 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 9 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 2$$

Théorème fondamental (Galois)

Th | 2 permutations de $S_n$ sont conjuguées dans $S_n$ ssi elles ont des décompositions en un même nbre de cycles de m̂ longueur.

ex : dans $S_9$

$$\sigma = (1\ 4\ 5)(2\ 3\ 7\ 8\ 9\ 6)$$

$\downarrow \alpha$ ... etc

$$\tau = (2\ 7\ 8)(1\ 5\ 4\ 3\ 9\ 6)$$

$\sigma$ et $\tau$ sont conjugués puisque $\exists \alpha \in S_9 \ / \ \alpha \sigma \alpha^{-1} = \tau$

Exercice 1 : Soit $\rho : G \to \mathrm{Aut}\, G$ . C'est un homomorphisme
$g \mapsto \varphi_g$

Montrer que $\mathrm{Ker}\, \rho = Z(G)$ (centre de G). En déduire que le centre d'un groupe est un sous-groupe distingué.

Montrer que $G/Z(G)$ est isomorphe à $\mathrm{Int}\, G$

Sol :

$\mathrm{Ker}\, \rho = \{ x \in G \ / \ \forall g \in G \quad g x g^{-1} = x \} = Z(G)$

$Z(G)$ est donc un s-groupe distingué. De plus, nous avons la décomposition canonique :

$$\begin{array}{ccc} G & \xrightarrow{\rho} & \mathrm{Aut}\, G \\ \pi \downarrow & & \uparrow i \\ G/Z(G) & \xrightarrow{\sim} & \mathrm{Int}\, G \end{array}$$

ce qui montre bien que $G/Z(G)$ et $\mathrm{Int}\, G$ sont isomorphes.

Exercice 2 : Montrer que tout automorphisme de $\mathcal{S}_3$ est intérieur.

Remarquons tout d'abord que $Z(\mathcal{S}_3) = \{1\}$. En effet, d'après l'exercice précédent :

$Z(\mathcal{S}_3)$ est distingué.

Or le seul s-groupe distingué de $\mathcal{S}_3$ est $\mathcal{A}_3$ (non trivial !)

Or : $\underbrace{(1\,2\,3)(2\,3)}_{1 \to 2} \neq \underbrace{(2\,3)\;(1\,2\,3)}_{1 \to 3} \Rightarrow Z(\mathcal{S}_3) = \{1\}$.

D'après l'exercice précédent : $\mathrm{Int}\,\mathcal{S}_3 \xrightarrow{\sim} \mathcal{S}_3$

c.à.d $\quad \mathrm{Card}\,\mathrm{Int}\,\mathcal{S}_3 = 6$.

Soit $\varphi \in \mathrm{Aut}\,\mathcal{S}_3$. Alors "$\varphi$ conserve l'ordre des éléments".

$(1\,2) \longrightarrow 3$ possibilités
$(2\,3) \longrightarrow 2$ "
$(1\,3) \longrightarrow 1$
} soit 6 possibilités.

Les images de $(1\,2\,3)$ et de $(1\,3\,2)$ sont déterminées par le choix ci-dessus [compte tenu de $(1\,2\,3) = (2\,3)(1\,3)$, et du fait que $\varphi$ soit un homomorphisme]. ↑ condition nécessaire pour que $\varphi \in \mathrm{Aut}\,\mathcal{S}_3$ !

Donc $\quad \mathrm{Card}\,\mathrm{Aut}\,\mathcal{S}_3 \underset{\triangle}{\leq} 6$

d'où $\quad \mathrm{Card}\,\mathrm{Int}\,\mathcal{S}_3 = 6 \leq \mathrm{Card}\,\mathrm{Aut}\,\mathcal{S}_3 \leq 6$.

$$\mathrm{Int}\,\mathcal{S}_3 = \mathrm{Aut}\,\mathcal{S}_3$$

CQFD

Actions de groupes

① Définition sur le polycoop

② Autre définition :

G opère à gauche sur X si :

$\exists \varphi : G \longrightarrow \mathcal{S}_X$

et $\varphi$ = homomorphisme (c.à.d $\varphi_{gg'} = \varphi_g \circ \varphi_{g'}$ si $\varphi_g = \varphi(g)$ )

Exemples :

* $GL(E) \times G_k(E) \longrightarrow G_k(E)$

où $G_k(E) = \{$ sous-e.v. de dimension $k \}$.

$GL(E)$ opère à gauche sur $G_k(E)$

* $G \times G \longrightarrow G$

$(g, h) \longmapsto g h g^{-1}$

Tout groupe G opère sur lui-même.

* $GL(E) \times E \longrightarrow E$ e.v.

$(f, x) \longmapsto f(x)$

opère non transitivement ...

- $Gx = \{ y \in X \ / \ \exists g \in G \ \ y = gx \}$ = orbite de $x$ sous G

- On dit que G opère sur X transitivement pour exprimer que :
  - * $G \backslash X$ a un seul élément
  - * $\forall x, x' \in X \quad \exists g \in G \ / \ x' = gx$
  - * Il n'y a qu'une seule orbite : $X = Gx$

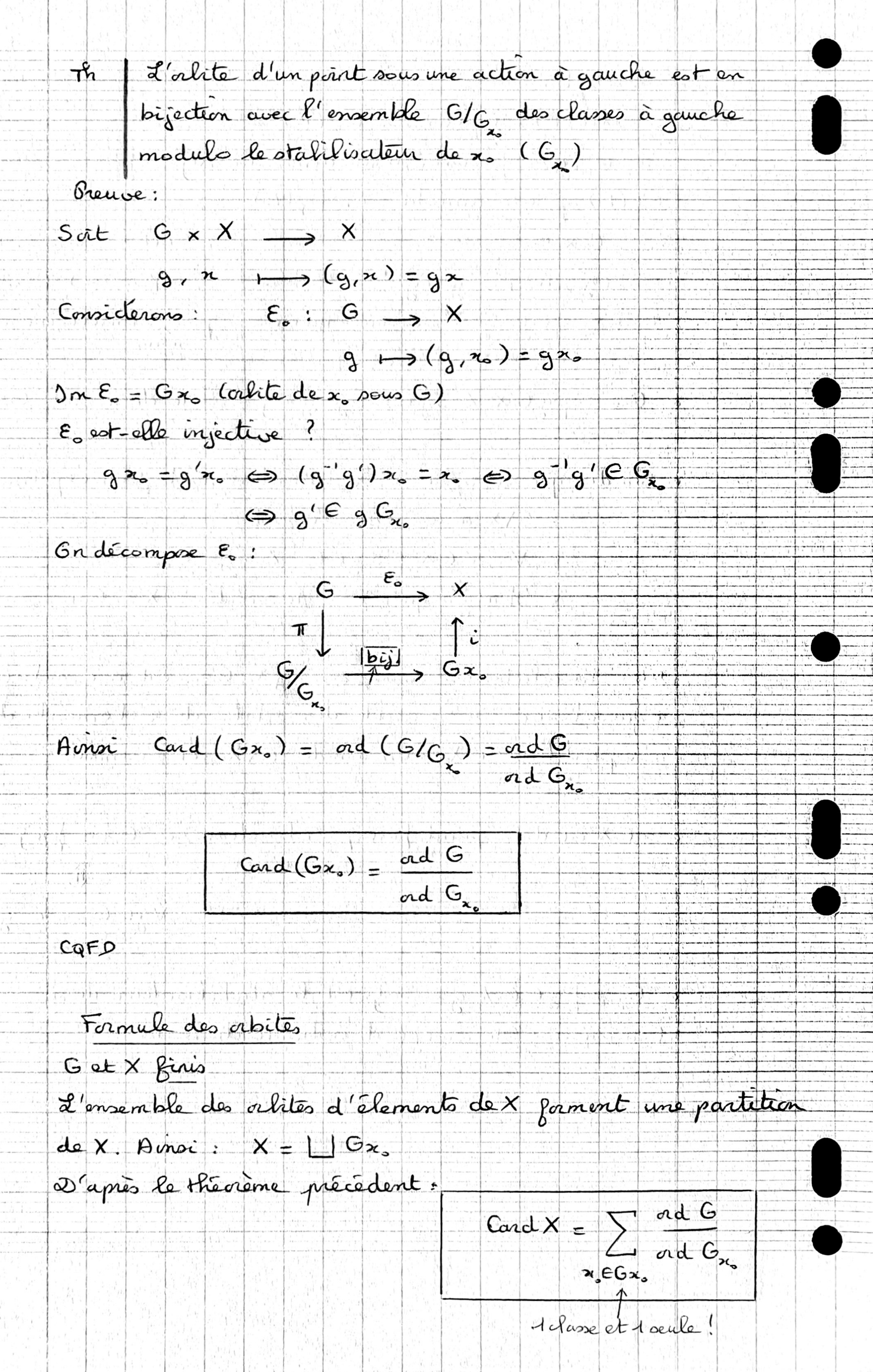
NB : la relation $x \mathcal{R} y \Leftrightarrow y \in Gx$ est une relation d'équivalence. L'ensemble des orbites des éléments de X forme une partition de X. On a noté $G \backslash X$ cet ensemble.

- $x \in X$ est dit "point fixe pour l'action" si $Gx = \{x\}$

$\Updownarrow$

$\forall g \in G \quad x = gx$

- $G_x = \{ g \in G \ / \ gx = x \}$ est le stabilisateur de $x$ (ou encore : "le groupe d'isotropie de $x$")



**Th** | L'orbite d'un point sous une action à gauche est en bijection avec l'ensemble $G/G_{x_0}$ des classes à gauche modulo le stabilisateur de $x_0$ ($G_{x_0}$)

Preuve :

Soit $G \times X \longrightarrow X$

$g, x \longmapsto (g, x) = gx$

Considérons : $\varepsilon_0 : G \longrightarrow X$

$g \longmapsto (g, x_0) = gx_0$

$\text{Im}\, \varepsilon_0 = Gx_0$ (orbite de $x_0$ sous $G$)

$\varepsilon_0$ est-elle injective ?

$gx_0 = g'x_0 \Leftrightarrow (g^{-1}g')x_0 = x_0 \Leftrightarrow g^{-1}g' \in G_{x_0}$

$\Leftrightarrow g' \in g\, G_{x_0}$

On décompose $\varepsilon_0$ :

$$\begin{array}{ccc} G & \xrightarrow{\varepsilon_0} & X \\ \pi \downarrow & & \uparrow i \\ G/G_{x_0} & \xrightarrow[\text{bij}]{} & Gx_0 \end{array}$$

Ainsi $\text{Card}\,(Gx_0) = \text{ord}\,(G/G_{x_0}) = \dfrac{\text{ord}\, G}{\text{ord}\, G_{x_0}}$

$$\boxed{\text{Card}(Gx_0) = \frac{\text{ord}\, G}{\text{ord}\, G_{x_0}}}$$

CQFD

## Formule des orbites

G et X finis

L'ensemble des orbites d'éléments de X forment une partition de X. Ainsi : $X = \bigsqcup Gx_0$

D'après le théorème précédent :

$$\boxed{\text{Card}\, X = \sum_{x_0 \in Gx_0} \frac{\text{ord}\, G}{\text{ord}\, G_{x_0}}}$$

↑ 1 classe et 1 seule !

## Groupe p-primaire

**Def** Soit $p>0$ un entier premier. On dit que $G$ est un p-groupe (ou un groupe "p-primaire") si

$$\text{ord}\, G = p^n \qquad (n \in \mathbb{N})$$

**Th** Soit $G$ un p-groupe. Alors son centre $Z(G)$ n'est pas réduit à l'élément neutre.

Preuve :

$Z(G) = \{$ ensemble des points fixes sous l'action de $G$ sur $G$ par automorphisme intérieur $\}$

$G = \bigsqcup$ (classes de conjugués)

On applique la formule des orbites en remarquant que :

$$G_g = G \iff \forall x \in G \quad gx = xg$$
$$\iff g \in Z(G)$$

d'où :

$$\text{ord}\, G = \sum_{g \in G_g} \frac{\text{ord}\, G}{\text{ord}\, G_g}$$

$$p^n = \text{ord}(Z(G)) + \sum_{\text{ord}\, G_g < p^n} \frac{\text{ord}\, G \leftarrow p^n}{\text{ord}\, G_g \leftarrow p^\alpha} \quad (\alpha \leq n)$$

$$p^n = \text{ord}(Z(G)) + \sum (\text{multiples de } p)$$

d'où :

$$\boxed{\# Z(G) \equiv 0 \quad [p]}$$

## 1°/ Recherche des sous-groupes distingués de $\mathcal{S}_n$

Th | Le seul sous-groupe distingué non trivial de $\mathcal{S}_n$ est le groupe alterné $\mathcal{A}_n$ si $n \neq 4$.

Idée de la démonstration :

- $\mathcal{S}_n$ engendré par $(i,j)$
- $\mathcal{A}_n$ " par les cycles de longueur 3 $(i,j,k)$
- Soit $G \triangleleft \mathcal{S}_n$ et $G \neq \{e\}$

On montre que $G$ contient au moins un élément de la forme $(i,j)$ ou $(i,j,k)$

Alors $G$ les contient tous, donc $\mathcal{A}_n \subset G$ ou $\mathcal{S}_n \subset G$.

Si $\mathcal{A}_n \subset G$, comme $ord(\mathcal{A}_n) = \frac{n!}{2}$

$ord(\mathcal{S}_n) = n!$

$$\frac{n!}{2} \mid ord(G) \mid n! \Rightarrow ord(G) = n! \text{ ou } \frac{n!}{2}$$

Ainsi $G = \mathcal{A}_n$ ou $\mathcal{S}_n$.

Si $\mathcal{S}_n \subset G$, alors $\mathcal{S}_n = G$.

Cas de $\mathcal{S}_4$

On a $\mathcal{S}_4 \triangleright \mathcal{A}_4 \triangleright K$     $K$ ≙ groupe de Klein

$K = \{1, (12)(34), (13)(24), (23)(14)\}$

De plus, $K \triangleleft \mathcal{S}_4$ car il est invariant par tout automorphisme intérieur de $\mathcal{S}_4$. (En effet, l'un quelconque des conjugués de $(12)(34)$ est dans $K$, puisqu'il est décomposable en 2 cycles de m̃ longueur)

Il n'y a pas d'autres sous-groupes distingués de $\mathcal{S}_4$.

Remarque :

* $G \triangleright H \triangleright K \not\Rightarrow K \triangleleft G$

contre-ex : $\mathfrak{A}_4 \triangleright K \supset \{\underbrace{1, (12)(34)}\}$

sous-groupe distingué de K

et pourtant $\{1, (12)(34)\}$ n'est pas distingué dans $\mathfrak{A}_4$.

En effet : $(123)[(12)(34)](123)^{-1} = (23)(14)$

* Par contre $G \triangleright H \triangleright\triangleright K \Rightarrow G \triangleright K$

où $H \triangleright\triangleright K$ signifie que K est invariant par tout automorphisme de H.

En effet, soit $\varphi_g$ un automorphisme intérieur de G, alors

$\varphi_g|_H$ = automorphisme de H

$\Downarrow$

$\begin{cases} \varphi_g|_H(K) = K \\ K \subset H \end{cases}$

$\Downarrow$

$\varphi_g(K) = K \Rightarrow K \triangleleft G$

2°/ Recherche des sous-groupes distingués de $\mathfrak{A}_n$

Même méthode qu'au 1°/

1/ Si $G \neq \{e\} \Rightarrow \exists (i,j,k) \in G$ ~~ou $\exists (i,j) \in G$~~

5

2/ $\exists (i,j,k) \in G \Rightarrow \forall (i,j,k)$ , $(i,j,k) \in G$

$\uparrow$

oui ssi $n \geq 5$

Th | $\mathfrak{A}_n$ $(n \geq 5)$ n'a pas de sous-groupes distingués non trivial.

# Groupes commutatifs finis

**Théorème :** Soit $G$ un groupe cyclique d'ordre $n$. $G = \langle x \rangle$

1) Tout sous-groupe $H$ de $G$ est cyclique (division euclidienne)

Si $k > 0$ est le plus petit entier tel que $x^k \in H$, alors $H = \langle x^k \rangle$.

$k$ divise $n$ et $\text{ord}(H) = \frac{n}{k}$

2) Si $H = \langle x^k, x^\ell \rangle$, alors $H = \langle x^\delta \rangle$ où $\delta = \Delta(k, \ell)$

3) Si $d$ divise $n$, $G$ possède un unique sous-groupe d'ordre $d$. Il est engendré par $x^{\frac{n}{d}}$.

(Bavier p45)

---

**Théorème :** $G$ et $G'$ deux groupes de cardinaux respectifs $n$ et $m$.

Alors $\left\{ G \times G' \text{ cyclique} \iff \left\{ \begin{array}{c} G \text{ cyclique} \\ \text{et} \\ G' \text{ cyclique} \end{array} \right\} \boxed{\text{ssi}} \ \Delta(m,n) = 1 \right.$

Preuve : (lemme : $\omega((x,y)) = \mu(\omega(x), \omega(y))$ )

$G \times G'$ cyclique $\iff \exists (x,y) \in G \times G' \ / \ \omega[(x,y)] = mn$

(si card $G = n$ et card $G' = m$)

Alors : $\omega[(x,y)] = mn \iff \mu(\omega(x), \omega(y)) = mn$ (1)

or $\omega(x) \mid n$
$\omega(y) \mid m$

donc (1) $\iff \begin{cases} \omega(x) = m \\ \omega(y) = n \\ \Delta(m,n) = 1 \end{cases}$ (simple calcul)

---

# GROUPE QUOTIENT

## I Groupe quotient

$\mathcal{R}$ = rel. d'∼ sur un groupe $G$

Def | $\mathcal{R}$ est compatible avec . ssi (∼) :
1) $\mathcal{R}$ est comp. à d. et à g. (c.à.d $x\mathcal{R}y \Rightarrow xa\mathcal{R}ya$ ..etc)
2) $\left.\begin{array}{l} x\mathcal{R}x' \\ y\mathcal{R}y' \end{array}\right\} \Rightarrow xy\mathcal{R}x'y'$

* Si $\mathcal{R}$ est compatible avec ., on peut définir le groupe $(G/\mathcal{R}, \cdot)$ où : $\dot{x}.\dot{y} = \dot{\overline{xy}}$

Inversement, si $(G/\mathcal{R}, .)$ = groupe, $\mathcal{R}$ est comp. avec .

## II Recherche de toutes les relations compatibles

1) Soit $\mathcal{R}$ compatible à droite avec .

$$x\mathcal{R}y \Leftrightarrow xy^{-1}\mathcal{R}e \Leftrightarrow xy^{-1} \in \dot{e}$$

$G$ $\dot{e}$ = sous-groupe de $G$

2) Inversement, soit $H$ s-groupe de $G$

Alors $x\mathcal{R}y \Leftrightarrow xy^{-1} \in H$ définit bien une relation d'équivalence, comp. à droite, et $\dot{x} = Hx$

Th | Sont ∼ :
1) $\mathcal{R}$ compatible à droite avec .
2) $\exists H$ s.groupe de $G$ / $x\mathcal{R}y \Leftrightarrow xy^{-1} \in H$

Equivalence des assertions :
1) $\mathcal{R}$ compatible avec .
2) $\mathcal{R}$ comp. à d et comp. à g.
3) $\exists H$ $x\mathcal{R}y \Leftrightarrow xy^{-1} \in H$
$\exists H'$ $x\mathcal{R}y \Leftrightarrow x^{-1}y \in H'$ (d'ailleurs : $H' = \dot{e} = H$)
4) $\exists H$ $x\mathcal{R}y \Leftrightarrow xy^{-1} \in H$ où $H \triangleleft G$

# DECOMPOSITION CANONIQUE

## I Décomposition canonique d'une application

$x \mathcal{R} y \Leftrightarrow f(x) = f(y)$

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \pi \downarrow & & \uparrow i \\ E/\mathcal{R} & \xrightarrow{\bar{f}} & \text{Im} f \end{array}$$

$\bar{f}$ bijective $(\bar{f}(\dot{x}) = f(x))$

## II Décomposition can. d'un homomorphisme de groupes

$(\text{Ker} f) \triangleleft G$

$x \mathcal{R} y \Leftrightarrow x y^{-1} \in \text{Ker} f$

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \pi \downarrow & & \uparrow i \\ (G/_{\text{Ker} f}, \cdot) & \xrightarrow{\bar{f}} & \text{Im} f \end{array}$$

($f$ homomorph. de groupes)

$\bar{f}$ = isomorphisme de groupes

## III Décomposition can. d'une appl. linéaire

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \pi \downarrow & & \uparrow i \\ (E/_{\text{Ker} f}, +, \cdot) & \xrightarrow{\bar{f}} & \text{Im} f \end{array}$$

($f$ appl. linéaire)

$\bar{f}$ = isomorphisme d'e.v.

# Groupes $(\mathbb{Z}/n\mathbb{Z},+)$ et $(\mathcal{U}(\mathbb{Z}/n\mathbb{Z}),\cdot)$

Plan d'étude : I Fonction indicatrice d'Euler

II Théorème chinois

1°/ Théorème chinois

2°/ Résolution du système $\begin{cases} x \equiv x_1 \ [a] \\ x \equiv x_2 \ [b] \end{cases}$

3°/ Algorithme d'Euclide

III Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

IV Caractérisation d'un groupe cyclique. Application.

1°/ Caractérisation

2°/ $\mathcal{U}(\mathbb{Z}/p\mathbb{Z})$ est cyclique quand $p$ premier.

---

## I Fonction indicatrice d'Euler.

On se propose d'étudier l'ensemble $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ des éléments multiplicativement inversibles de $\mathbb{Z}/n\mathbb{Z}$. Donnons un théorème fondamental :

**Th** Soit $\dot{m} \in \mathbb{Z}/n\mathbb{Z}$ $(0 \leq m < n)$. Les 3 propriétés suivantes sont équivalentes :

i) $\Delta(m,n) = 1$

ii) $\dot{m} \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$, ensemble des él. mult. inversibles de $\mathbb{Z}/n\mathbb{Z}$

iii) $\dot{m}$ engendre le groupe $\mathbb{Z}/n\mathbb{Z}$

Preuve :

i) $\Leftrightarrow$ ii) $\Delta(m,n) = 1 \Leftrightarrow \exists u, v \in \mathbb{Z} \quad mu + nv = 1$ (Bezout)

$\Leftrightarrow \exists u \in \mathbb{Z} \ / \ \dot{m}\dot{u} = \dot{1}$ (dans $\mathbb{Z}/n\mathbb{Z}$)

$\Leftrightarrow \dot{m} \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$

i) $\Leftrightarrow$ iii) $\quad \Delta(m,n)=1 \Leftrightarrow \exists u,v \in \mathbb{Z} \quad mu+nv=1$ (Bezout)

$\Leftrightarrow \exists u \in \mathbb{Z} \,/\, u\dot{m}=\dot{1}$ (dans $\mathbb{Z}/n\mathbb{Z}$)

$\Leftrightarrow \dot{1} \in \langle \dot{m} \rangle$

$\Leftrightarrow \langle \dot{m} \rangle = \mathbb{Z}/n\mathbb{Z}$ (car $\dot{1}$ = él. gén. de $\mathbb{Z}/n\mathbb{Z}$)

CQFD

Problème : Combien y-a-t'il d'éléments multiplicativement inversibles dans $\mathbb{Z}/n\mathbb{Z}$ ?
Soit $\varphi(n)$ ce nombre. Il est fini.

$\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}$ est la "fonction indicatrice d'Euler"

Trouver $\varphi(n)$ pour tout $n \in \mathbb{N}^*$ ?

a) Si $p$ premier, $\mathcal{U} = \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \Rightarrow \varphi(p) = p-1$ $\quad \varphi(1) = 1$

Th | $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ = corps $\Leftrightarrow$ $n$ premier

b) Recherche de $\varphi(p^n)$ où $p$ premier.

* lemme : Soit $p$ premier, et $n \in \mathbb{N}^*$. Alors $a | p^n \Rightarrow a \in \{1, p, \dots, p^n\}$

Preuve : récurrence sur $n$.

- Pour $n=1$ : $\exists! a = p$ ou $1$ qui divise $p$
- Vrai pour $n \Rightarrow$ vrai pour $n+1$ ?

$a | p^{n+1} \Leftrightarrow a | p.p^n$

- $\rightarrow p | a \Rightarrow a = a_1 p \Rightarrow a_1 | p^n \Rightarrow a_1 \in \{1, \dots, p^n\}$ donc $a \in \{p, \dots, p^{n+1}\}$
- $\rightarrow p \nmid a \Rightarrow \Delta(a,p) = 1 \Rightarrow a | p^n \Rightarrow \begin{cases} a \in \{1, \dots, p^n\} \\ \text{et } p \nmid a \end{cases} \Rightarrow a = 1$

CQFD

* Cherchons maintenant tous les éléments inversibles de $\mathbb{Z}/p^n\mathbb{Z}$

$$\mathbb{Z}/p^n\mathbb{Z} = \{0, 1, 2, \dots, p^n - 1\}$$

On a la propriété (1) : Si $0 < a < p^n$, alors $\Delta(a, p^n) = 1 \Leftrightarrow a \neq kp \quad (k \in \mathbb{Z})$

En effet : ($\Rightarrow$) oui

($\Leftarrow$) Si $a \neq kp$, soit $\delta | p^n \Rightarrow \delta \in \{1, \dots, p^n\}$ (cf lemme)

Si $\delta = p^\alpha$ ($\alpha \in [1,n]$), alors $p^\alpha | a \Rightarrow \exists k \,/\, a = kp^\alpha = (kp^{\alpha-1})p$ (si $\alpha \geq 1$) absurde.

Donc $\alpha = 0 \Rightarrow \delta = 1 = \Delta(a, p^n)$ CQFD

* Combien y-a-t'il d'éléments de la forme $kp$ dans $]0, p^n[$ ?

$0 < kp < p^n \Leftrightarrow 0 < k < p^{n-1}$ soit $p^{n-1} - 1$ possibilités pour $k$.

Ainsi, dans $\{1, 2, \dots, p^n - 1\}$ il y a $p^{n-1} - 1$ et seulement $p^{n-1} - 1$ nombres tels que

$\Delta(a, p^n) \neq 1 \Leftrightarrow$ il y a, dans cette liste, exactement $p^{n-1} - 1$ nombres $\notin \mathcal{U}$

N'oublions pas $0 \notin \mathcal{U}$. Dans $\{0, \dots, p^n - 1\}$, il y a exactement $p^{n-1}$ nombres $\notin \mathcal{U}$

Donc $\varphi(p^n) = \text{Card}(\mathcal{U}) = \text{ord}(\mathcal{U}) = p^n - p^{n-1}$

$$\boxed{\varphi(p^n) = (p-1)p^{n-1}}$$

c) $\forall n \in \mathbb{N}$ $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ où $p_i$ $(1 \leq i \leq r)$ sont des entiers premiers distincts $(\alpha_i \in \mathbb{N}^*)$

Pour connaître $\varphi(n)$, il nous suffirait de savoir que :

$$\forall a, b \ / \ \Delta(a, b) = 1 \quad : \quad \varphi(ab) = \varphi(a)\varphi(b) \qquad (1)$$

Alors $\varphi(n) = \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$

(1) signifie que les anneaux $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ ont m̂ nbre d'éléments inversibles.

En fait, nous allons voir (au II) que ces anneaux sont <u>isomorphes</u>, ce qui sera une <u>condition suffisante</u> pour avoir (1)

Alors, nous aurons :

$$\boxed{\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)}$$

## II Théorème chinois

### 1°/ <u>Théorème chinois</u>

| | |
|---|---|
| Th | $a, b \in \mathbb{N}$ $\underline{\Delta(a, b) = 1}$<br>Alors $\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ en tant qu'<u>anneaux</u>. |

Preuve :

Considérons $f : \mathbb{Z} \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, $z \longmapsto (\dot{z}, \bar{z})$. Montrons que c'est un morphisme d'anneaux, et que $\text{Ker} f = a\mathbb{Z} \cap b\mathbb{Z} = ab\mathbb{Z}$ (car $\mu = ab$)

- $f$ est un morphisme pour les lois + et .

$$\begin{cases} f(z+z') = (\dot{z}+\dot{z}', \bar{z}+\bar{z}') = f(z)+f(z') \\ f(zz') = f(z).f(z') \end{cases}$$

- $\operatorname{Ker} f = ab\mathbb{Z}$

$$z \in \operatorname{Ker} f \Leftrightarrow \begin{cases} \dot{z} = \dot{0} \\ \bar{z} = \bar{0} \end{cases} \Leftrightarrow z \in a\mathbb{Z} \cap b\mathbb{Z} = ab\mathbb{Z} \quad (\text{car } \mu = ab)$$

- $ab\mathbb{Z}$ = idéal de $\mathbb{Z}$ $\Rightarrow$ on peut parler d'anneaux $(\mathbb{Z}/ab\mathbb{Z}, +, .)$ et :

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ \pi \downarrow & \nearrow \tilde{f} & \\ \mathbb{Z}/ab\mathbb{Z} & & \end{array} \qquad (I)$$

- Dans le diagramme (I), $\tilde{f}$ admet $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ pour but car $f$ est surjective.

En effet : $\forall \dot{x} \in \mathbb{Z}/a\mathbb{Z}$
$\forall \bar{y} \in \mathbb{Z}/b\mathbb{Z}$ $\quad \exists z \in \mathbb{Z} / \begin{cases} \dot{z} = \dot{x} \\ \bar{z} = \bar{y} \end{cases}$

puisque le système en $z$ : $\begin{cases} z \equiv x \ [a] \\ z \equiv y \ [b] \end{cases}$ admet au moins une solution, eu égard au fait que $\delta(a,b) = 1$. (voir 2°/)

Remarque : Montrer la réciproque.

contraposée : Si $\delta(a,b) = \delta \neq 1 \Rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \not\simeq \mathbb{Z}/ab\mathbb{Z}$. En effet $\mu\delta = ab \Rightarrow \mu < ab$
or, $\forall (\dot{x}, \bar{y}) \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ $\quad \mu(\dot{x}, \bar{y}) = (\mu\dot{x}, \mu\bar{y}) = (\dot{0}, \bar{0}) \Rightarrow$ tout élément de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est au plus d'ordre $\mu < ab \Rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \not\simeq \mathbb{Z}/ab\mathbb{Z}$.

NB : Ainsi $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ cyclique $\Leftrightarrow \delta(a,b) = 1$

Généralisation aisée par récurrence

Th | $a_1, \dots, a_n \in \mathbb{N}$ premiers entre eux 2 à 2
Alors $\mathbb{Z}/a_1 \dots a_n\mathbb{Z} \simeq \mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_n\mathbb{Z}$

2°/ Résolution du système $\begin{cases} x \equiv x_1 \ [a] \\ x \equiv x_2 \ [b] \end{cases}$ (I)

$$(I) \Leftrightarrow \exists k, k' \in \mathbb{Z} / \begin{cases} x = x_1 + ka \\ x = x_2 + k'b \end{cases}$$

$$\Leftrightarrow \exists k, k' \in \mathbb{Z} / x = x_1 + ka \text{ et } \quad ka - k'b = x_2 - x_1$$

* Si $\Delta(a,b) \nmid x_2 - x_1$ , $S = \emptyset$

* Si $\Delta(a,b) \mid (x_2 - x_1)$ , posons $\Delta(a,b) = \delta$. On est amenés à résoudre

$$\begin{cases} k\left(\frac{a}{\delta}\right) - k'\left(\frac{b}{\delta}\right) = \frac{x_2 - x_1}{\delta} \\ \Delta\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = 1 \end{cases}$$

Simplifions les écritures et résolvons (1) $ka - k'b = x_2 - x_1$ où $\Delta(a,b) = 1$

On connait une solution particulière de (1) (voir, par exemple, l'algorithme d'Euclide au 3%). En effet :

$$\exists u_0, v_0 \ / \ u_0 a + v_0 b = 1$$

(cf. Bezout)

$$\Downarrow$$

$$\underbrace{u_0(x_2 - x_1)}_{u} a + \underbrace{v_0(x_2 - x_1)}_{v} b = (x_2 - x_1)$$

$$(1) \Leftrightarrow \begin{cases} ka - k'b = x_2 - x_1 \\ ua + vb = x_2 - x_1 \end{cases}$$

$$(k - u)a = (k' + v)b \qquad (2)$$

$$\begin{cases} a \mid (k' + v)b \\ \text{et} \\ \Delta(a,b) = 1 \end{cases} \Longrightarrow (\text{gauss}) \quad a \mid (k' + v) \Rightarrow \exists q \in \mathbb{Z} \ / \ k' + v = qa$$

Alors (2) donne $(k - u)\cancel{a} = q\cancel{a}b \Leftrightarrow k = u + qb$

Ainsi $(1) \Leftrightarrow \begin{cases} k = u + qb \\ k' = -v + qa \end{cases} \quad (q \in \mathbb{Z})$

on a procédé par équivalences ! le vérifier

Inversement, $\forall q \in \mathbb{Z}$ $\begin{cases} k = u + qb \\ k' = -v + qa \end{cases} \Rightarrow ka - k'b = x_2 - x_1 \Rightarrow (k, k')$ sol. de (1)

L'ensemble des solutions de (I) est donc :

$$S = \{ x = x_1 + (u + qb)a \ / \ q \in \mathbb{Z} \}$$

$$\begin{cases} x \equiv x_1 \ [a] \\ x \equiv x_2 \ [b] \end{cases}$$

$\rightarrow \Delta(a,b) \nmid (x_2 - x_1)$ $S = \emptyset$

$\rightarrow \Delta(a,b) \mid (x_2 - x_1)$ $S$ infini

3°/ Algorithme d'Euclide [pour la recherche d'une sol. particulière de l'équation $x_1 + au = x_2 + bv$ X $au - bv = 1$]

a) Rappel : détermination pratique du PGCD

Soient $a, b \in \mathbb{Z} \times \mathbb{Z}^*$. Si $a = bq_1$ ($q_1 \in \mathbb{Z}$) alors $\Delta(a,b) = |b|$

sinon, on utilise l'algorithme d'Euclide

(a)
$$\begin{cases} a = bq_1 + r_1 & \text{et } \Delta(a,b) = \Delta(b, r_1) \\ b = r_1 q_2 + r_2 & \Delta(b, r_1) = \Delta(r_1, r_2) \\ r_1 = r_2 q_3 + r_3 & \Delta(r_1, r_2) = \Delta(r_2, r_3) \\ \text{-------} & \text{-------} \\ r_{k-2} = r_{k-1} q_k + r_k & \Delta(r_{k-2}, r_{k-1}) = \Delta(r_{k-1}, r_k) \\ r_{k-1} = r_k q_{k+1} & \Delta(r_{k-1}, r_k) = \Delta(r_k, 0) = r_k \end{cases}$$

Cet algorithme aboutira certainement puisqu'il n'y a qu'un nombre fini de naturels entre $|b|$ et 0, et que $\forall k \in \mathbb{N}$ $\quad 0 \leq r_{k+1} < r_k < |b|$

Ainsi

|| $\Delta(a,b)$ = dernier reste non nul dans l'algorithme d'Euclide

b) Application : cet algorithme donne une solution particulière de l'équ. de Bezout $au + bv = 1$

En effet :

$$au + bv = 1$$

* Si $\Delta(a,b) \neq 1$, $\nexists$ solution
* Si $\Delta(a,b) = 1$, $\exists$ solutions

Dans ce cas, l'algorithme (a) donne $r_k = 1$

$$\begin{cases} a = bq_1 + r_1 & \Rightarrow r_1 = a - bq_1 \doteq \alpha_1 a + \beta_1 b \\ b = r_1 q_2 + r_2 & \Rightarrow r_2 = b - r_1 q_2 = b - (a - bq_1) q_2 \doteq \alpha_2 a + \beta_2 b \\ \text{-------------} & \\ r_{k-3} = r_{k-2} q_{k-1} + r_{k-1} & \Rightarrow r_{k-1} = \alpha_{k-1} a + \beta_{k-1} b \quad \text{(récurrence)} \end{cases}$$

$$r_{k-2} = r_{k-1} q_k + 1 \Rightarrow 1 = r_{k-2} - r_{k-1} q_k = \alpha_{k-2} a + \beta_{k-2} b - (\alpha_{k-1} a + \beta_{k-1} b) q_k$$

$$1 = \alpha a + \beta b \quad \text{oui.}$$

↑ ↑

# III Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

**Pro** Si $d$ divise $n$, alors il existe un unique sous-groupe d'ordre $d$ de $\mathbb{Z}/n\mathbb{Z}$, à savoir $\{\dot{0}, \dot{\frac{n}{d}}, ..., (d-1)\dot{\frac{n}{d}}\} = C_{\frac{n}{d}} \simeq \mathbb{Z}/d\mathbb{Z}$

Preuve :

- existence : Considérons l'ensemble des solutions de $d\dot{x} = \dot{0}$

$$d\dot{x} = \dot{0} \Leftrightarrow dx = kn \Leftrightarrow x = k\frac{n}{d} \quad (\text{car } d|n)$$

Ainsi $S = \{0, \dot{\frac{n}{d}}, ..., (d-1)\dot{\frac{n}{d}}\}$ = sous-groupe d'ordre $d$ de $\mathbb{Z}/n\mathbb{Z}$

- unicité Soit $G \subset \mathbb{Z}/n\mathbb{Z}$ un sous-groupe d'ordre $d$.

$\forall \dot{x} \in G \quad d\dot{x} = \dot{0} \Rightarrow \dot{x} \in S$ donc $G \subset S$ et $\text{ord}\, G = \text{ord}\, S \Rightarrow G = S$

## Application :

**Pro** On a la relation $$\boxed{\sum_{d|n} \varphi(d) = n}$$

Preuve :

* Combien y-a-t'il d'éléments d'ordre $d$ dans $\mathbb{Z}/n\mathbb{Z}$ ?

$\dot{x}$ d'ordre $d \Leftrightarrow \langle \dot{x} \rangle = C_{\frac{n}{d}} \Leftrightarrow x$ générateur de $C_{\frac{n}{d}}$ ("sous-groupe eng. par $\dot{\frac{n}{d}}$)

Or $C_{\frac{n}{d}} \simeq \mathbb{Z}/d\mathbb{Z} \Rightarrow$ il y a $\varphi(d)$ générateurs de $C_{\frac{n}{d}}$

Il y a donc $\varphi(d)$ éléments d'ordre $d$.

* Faisons une partition des $n$ éléments de $\mathbb{Z}/n\mathbb{Z}$ suivant leurs ordres $d$ (divisent $n$)

D'où $\sum_{d|n} \varphi(d) = n$

### Remarque

Cette formule permet de calculer $\varphi(n)$ par récurrence :

$$\varphi(6) = 6 - \underbrace{\varphi(2)}_{1} - \underbrace{\varphi(3)}_{2} - \underbrace{\varphi(1)}_{=1 \text{ (par définition)}}$$

## IV Caractérisation d'un groupe cyclique - Application

### 1°/ Caractérisation d'un groupe cyclique

(NB : on peut supprimer l'hyp. "abélien")

**Th** | Soit $(G,+)$ un groupe abélien d'ordre $n$.
G est cyclique ssi $\forall d$ diviseur de $n$ $\quad \text{ord}\{x\in G / dx = 0\} \leq d$

($G_d$ = éléments d'exposant d) $\quad \Gamma_d \subset G_d$

($\Rightarrow$) G cyclique $\Rightarrow$ G isomorphe à $\mathbb{Z}/n\mathbb{Z} \Rightarrow \{x \in G / dx = 0\} \simeq C_{\frac{n}{d}}$ et $\text{ord}\, C_{\frac{n}{d}} = d$

($\Leftarrow$) Soit $G = \Gamma_1 \cup \Gamma_2 \cup \dots \cup \Gamma_d \dots$ la partition de G, où $\Gamma_d = \{x \in G / x \text{ d'ordre } d\}$

Si $\Gamma_d \neq \emptyset$, $\exists x$ d'ordre d et $\langle x \rangle = \{0, x, \dots, (d-1)x\} \subset \{x \in G / dx = 0\}$

$\text{ord}\langle x\rangle = d$ et $\text{ord}\{x\in G / dx = 0\} \leq d$ montrent alors que $\langle x \rangle = \{x \in G / dx = 0\}$ (*)

Mais alors : y d'ordre d $\Leftrightarrow$ y engendre $\langle x \rangle \simeq \mathbb{Z}/d\mathbb{Z}$

Il y a $\varphi(d)$ générateurs de $\mathbb{Z}/d\mathbb{Z}$, il y aura donc $\varphi(d)$ éléments y d'ordre d dans G.

Ainsi : $\quad n = \sum_{d|n} \text{ord}(\Gamma_d) = \sum_{d|n} \varepsilon_d \varphi(d) \quad$ où $\begin{cases} \varepsilon_d = 0 & \text{si } \Gamma_d = \emptyset \\ \varepsilon_d = 1 & \text{si } \Gamma_d \neq \emptyset \end{cases}$

Or : $\sum_{d|n} \varphi(d) = n \Rightarrow \sum_{d|n} \varepsilon_d \varphi(d) = \sum_{d|n} \varphi(d) \Rightarrow \varepsilon_d = 1 \quad \forall d$ diviseur de $n$

D'où : $\underline{\forall d|n} \quad \underline{\Gamma_d \neq \emptyset}$

En particulier pour $d = n$, il existe au moins un élément générateur de G.
Donc G est cyclique.

CQFD

**Co** | Tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

(NB : on peut supprimer l'hypothèse "commutatif")

Preuve :

Soit $G \subset \mathbb{C}^*$, G fini.

Alors $x \in G \subset \mathbb{C}^* \quad \text{ord}\{x \in G / x^d = 1\} = \text{ord}\{x \in G / x^d - 1 = 0\}$

$\leq d$ (cf polynôme de degré d dans un corps commutatif !) | anneau comm. intègre

On applique le th. précédent.

## 2°/ Application : $\mathcal{U}(\mathbb{Z}/p\mathbb{Z})$ est cyclique quand $p$ premier.

**Th** | $\sim$
1) $\mathbb{Z}/n\mathbb{Z}$ est intègre
2) $\mathbb{Z}/n\mathbb{Z}$ est un corps
3) ~~$\mathbb{Z}/n\mathbb{Z}$~~ $n$ est premier

(laissé au lecteur)

**Co** | Soit $p$ premier. Alors $\mathcal{U}(\mathbb{Z}/p\mathbb{Z})$ est cyclique.

$\mathbb{Z}/p\mathbb{Z}$ est un corps fini, et $\mathcal{U}(\mathbb{Z}/p\mathbb{Z})$ est un groupe multiplicatif de ce corps.
Ainsi $((\mathbb{Z}/7\mathbb{Z})^*, .)$ est cyclique. L'un de ses générateurs est $\dot{3}$

$$\langle \dot{3} \rangle_\times = \{ \dot{3}, \dot{3}^2, = \dot{2}, \dot{6}, \dot{4}, \dot{5}, \dot{1} \} = \mathcal{U}(\mathbb{Z}/7\mathbb{Z})$$

# Supplements (F1)

## Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

$\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

Soit G un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$, alors $\pi^{-1}(G)$ est un sous-groupe de $\mathbb{Z}$ contenant $\pi^{-1}(\dot{0}) = n\mathbb{Z}$. Posons $\pi^{-1}(G) = d\mathbb{Z} \supset n\mathbb{Z}$ (1)

Nous aurons $\pi(d\mathbb{Z}) = G$ (car $\pi$ est surjective)

Pro | Il existe une bijection entre les diviseurs de n (d) et les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ $(\pi(d\mathbb{Z}))$

Preuve :

- A chaque diviseur de n on fait correspondre le sous-groupe $\pi(d\mathbb{Z}) \subset \mathbb{Z}/n\mathbb{Z}$
- Cette application est surjective par construction (cf(1))
- Est-elle injective ?

Montrons que $\left.\begin{matrix} \pi(d\mathbb{Z}) = \pi(d'\mathbb{Z}) \\ d|n \text{ et } d'|n \end{matrix}\right\} \Rightarrow d = d'$

Nous avons : $\pi(d) \in \pi(d'\mathbb{Z}) \Leftrightarrow \exists a \in \mathbb{Z} \ / \ d - d'a \in n\mathbb{Z}$
$\Leftrightarrow \exists a \ \exists b \ / \ d - d'a = bn$

or $\left.\begin{matrix} d'|n \Rightarrow d'|d \\ \text{de m̂ : } \quad d|d' \end{matrix}\right\} \Rightarrow d = d'$ oui

Remarque : $\pi(d\mathbb{Z}) = \{\xi \in \mathbb{Z}/n\mathbb{Z} \ / \ \exists x \in \mathbb{Z} \ \ \xi = d\dot{x}\}$
$= d(\mathbb{Z}/n\mathbb{Z})$
$\simeq \mathbb{Z}/\frac{n}{d}\mathbb{Z}$

Généralisation : Si $H \lhd G$

Pro | Soit $H \subset G$. Il existe une bijection croissante entre les sous-groupes de $G/H$ et les sous-groupes de G contenant H.

# 2 Groupes abéliens de type fini

## Groupe des entiers naturels $\mathbb{N}$

$\mathbb{N}$ est un ensemble non vide ($0 \in \mathbb{N}$)

(n1) bien ordonné (on pose $0 = \operatorname{Inf} \mathbb{N}$)

(n2) non majoré

(n3) tel que tout élément, sauf 0, a un prédecesseur.
(il est unique)

"bien ordonné" : $\forall F \subset E \quad F \neq \emptyset \quad \exists f \in F$ $f$ plus petit élément de $F$

Remarque : bien ordonné $\Rightarrow$ totalement ordonné
(considérer $\{a, b\} \subset \mathbb{N}$)

successeur : $e \in \mathbb{N} \qquad e+1 = \operatorname{Inf}\{e' \in \mathbb{N} \,/\, e' > e\}$
prédecesseur. (existe

Unicité de $\mathbb{N}$
Soient 2 ensembles vérifiant les axiomes n1 n2 n3. Alors il existe une bijection croissante entre eux, autrement dit, ces 2 ensembles définissent la même chose à une bijection près.

Existence de $\mathbb{N}$
Impossibilité de la démontrer (gödel)

Principe de récurrence

Th | Soit $E \subset \mathbb{N}$ vérifiant $\begin{cases} * \ 0 \in E \\ * \ n \in E \Rightarrow n+1 \in E \end{cases}$. Alors $E = \mathbb{N}$

Posons $\bar{E} = \mathbb{N} \setminus E$. De 2 choses l'une :

- Si $\bar{E} = \emptyset$, c'est fini
- Si $\bar{E} \neq \emptyset$, $\exists\, e = \text{Inf}\{\bar{E}$

$e \neq 0$ car $0 \in E$, donc $e$ admet un prédecesseur $e' \notin \bar{E}$

Mais $e' \in E \Rightarrow e'+1 = e \in E$

et $e \in E \cap \bar{E} \Leftrightarrow e \in \emptyset$, absurde.

<u>Remarque</u> : Considérons $\mathbb{N} \cup \{\omega\}$
et : $\forall n \in \mathbb{N} \quad n < \omega$. On obtient ainsi un autre ensemble bien ordonné.

Th | Soient X et Y deux ensembles bien ordonnés. Il existe une "bijection" croissante ("isomorphisme d'ensembles bien ordonnés") de X sur $]\leftarrow, y[ \subset Y$ ou de Y sur $]\leftarrow, x[$.

(injection → "bijection")

<u>Axiome de Zermelo</u>

Ax 1 | Tout ensemble peut être muni d'une relation de bon ordre.

Axiome du choix

Ax 2 | Soit $(X_i)_{i \in I}$ une famille de parties ($\forall i \in I \quad X_i \neq \emptyset$)
Il existe ~~la~~ une suite $(x_i)_{i \in I}$ / $x_i \in X_i \quad (\forall i \in I)$

$Ax1 \Rightarrow Ax2$ $\forall i$, on pose $\inf X_i = x_i \in X_i$
On obtient

En fait, on a $Ax1 \Leftrightarrow Ax2$ (admis)

→ L'ensemble $2^{\mathbb{N}} = \{u : \mathbb{N} \to \{0,1\}\}$ n'est pas en bijection avec $\mathbb{N}$.
2 façons de le démontrer :
1) $n \overset{\varphi}{\longmapsto} u^n$ $u^n = \{u_0^n, u_1^n, \ldots, \ldots\}$ $u_i^n = 0,1$

$$\begin{aligned} u^0 &= \{u_0^0, u_1^0, \ldots\} \\ u^1 &= \{u_0^1, u_1^1, u_2^1, \ldots\} \\ &\ldots\ldots\ldots \\ u^n &= \{u_0^n, u_1^n, u_2^n, \ldots\} \end{aligned} \quad (I)$$

Montrons que $\varphi$ n'est pas bijective : pour cela, considérons la suite $v \in 2^{\mathbb{N}}$ formée des termes diagonaux du tableau (I)

$$v : \mathbb{N} \to \{0,1\}, \quad p \mapsto v_p = \overline{u_p^p}$$

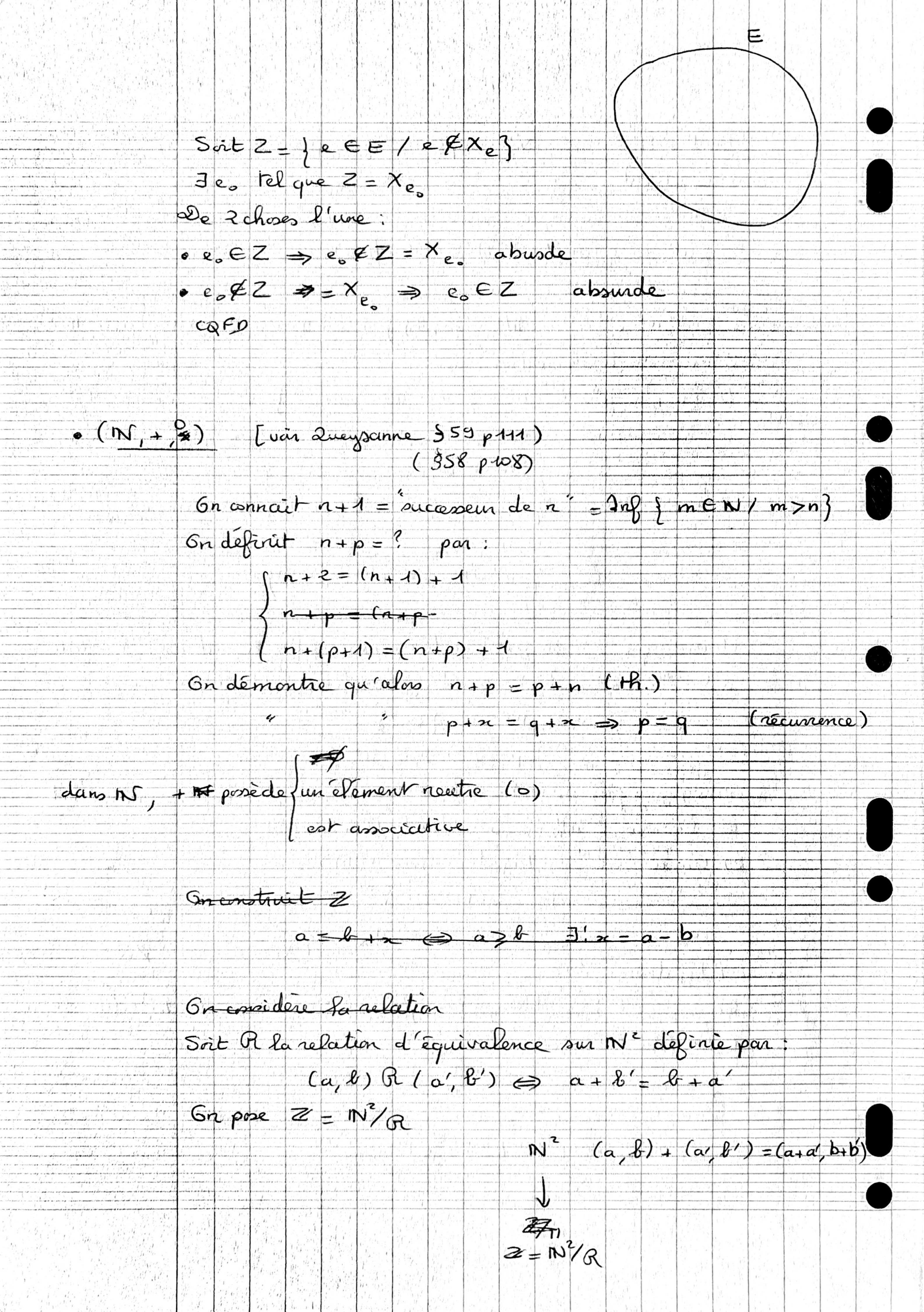
$v$ ne figure pas dans la liste (I), car sinon $v = u^N \Rightarrow v_N = u_N^N$
Or $v_N = \overline{u_N^N}$ ⇒ contradiction
2) On a : $2^{\mathbb{N}}$ en bijection avec $\mathcal{P}(\mathbb{N})$

$$\varphi : \mathcal{P}(\mathbb{N}) \to 2^{\mathbb{N}}, \quad X \mapsto \chi_X \quad \begin{cases} \chi_X(x) = 1 \text{ si } x \in X \\ \chi_X(x) = 0 \text{ si } x \notin X \end{cases}$$

$\varphi$ bijective.
Or, pour E ensemble quelconque, il n'existe pas de bijection de E sur $\mathcal{P}(E)$

$$E \not\rightleftarrows \mathcal{P}(E)$$

↓
Preuve
Si $\varphi : E \to \mathcal{P}(E)$ et $\varphi$ bijective,
$e \mapsto X_e$




Soit $Z = \{ e \in E \,/\, e \notin X_e \}$

$\exists e_0$ tel que $Z = X_{e_0}$

De 2 choses l'une :

- $e_0 \in Z \Rightarrow e_0 \notin Z = X_{e_0}$ abusde
- $e_0 \notin Z \Rightarrow = X_{e_0} \Rightarrow e_0 \in Z$ absurde

CQFD

- $(\mathbb{N}, +, \times)$ [voir Queysanne §59 p111)
  (§58 p108)

On connaît $n+1$ = "successeur de $n$" $= \text{Inf}\{ m \in \mathbb{N} \,/\, m > n \}$

On définit $n+p = ?$ par :

$$\begin{cases} n+2 = (n+1)+1 \\ \sout{n+p = (n+p-} \\ n+(p+1) = (n+p)+1 \end{cases}$$

On démontre qu'alors $n+p = p+n$ (th.)

" " $p+x = q+x \Rightarrow p = q$ (récurrence)

dans $\mathbb{N}$, + possède { un élément neutre (0)
est associative

~~On construit $\mathbb{Z}$~~

$a = \sout{b + x \Leftrightarrow a \geq b}$ $\exists!\, x = a - b$

~~On considère la relation~~

Soit $\mathcal{R}$ la relation d'équivalence sur $\mathbb{N}^2$ définie par :

$$(a, b)\, \mathcal{R}\, (a', b') \Leftrightarrow a + b' = b + a'$$

On pose $\mathbb{Z} = \mathbb{N}^2/\mathcal{R}$

$\mathbb{N}^2$ $(a, b) + (a', b') = (a+a', b+b')$

↓

$\mathbb{Z} = \mathbb{N}^2/\mathcal{R}$

$\mathbb{Z}$ = entiers rationnels est un groupe pour +.

$$\mathbb{N} \overset{\Phi}{\hookrightarrow} \mathbb{Z} = \mathbb{N}^2/\mathcal{R} \qquad \Phi \text{ est injective}$$
$$n \longmapsto \overline{(n, 0)}$$

On plonge $\mathbb{N}$ dans $\mathbb{Z}$ : $(n, 0)$ "=" $n$

$(0, n)$ "=" $-n$

$(0, 0)$ "=" $0$

On définit la multiplication par $\begin{cases} 0 . p = 0 \\ ~~n . 0 = 0~~ \\ 1 . p = p \\ n p = (n-1) p + p \\ ~~n p = n(p-1) + n~~ \end{cases}$ dans $\mathbb{N}$

Problème : Étendre, de la même façon, la multiplication de $\mathbb{N}$ à $\mathbb{Q}$.

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$

dans $\mathbb{Z}$ $\begin{cases} (-p) q = p(-q) = (-p)(-q) = -(pq) \\ \text{(règle des signes)} \end{cases}$

dans $\mathbb{Q} = \mathbb{Z}^2/_{\mathcal{R}}$ où $(a, b) \mathcal{R} (a', b') \Leftrightarrow ab' = ba'$

- $A$ = anneau commutatif intègre.

Th et Def On considère $A \times (A \setminus \{0\})$ et la relation

$(a, b) \mathcal{R} (a', b') \Leftrightarrow ab' = ba'$

C'est une relation d'équivalence.

On défini + sur $A \times (A \setminus \{0\})$ par $\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$

$(a, b) + (a', b') = (ab' + a'b, bb')$

× par : $(a, b) \times (a', b') = (aa', bb')$

Ces 2 lois sont compatibles avec la relation $\mathcal{R}$. On peut donc définir les lois internes + et × sur $A \times (A \setminus \{0\}) / \mathcal{R}$.
On vérifie que cet ensemble quotient est alors un corps.

Propriété universelle de K

$$\begin{array}{ccc} A & \hookrightarrow & K \\ a & \longmapsto & \overline{(a,1)} \end{array}$$

Soit K' un corps et $j : A \hookrightarrow K'$ un homomorphisme injectif d'anneaux.
Alors $K \subset K'$

$$\begin{array}{ccc} A & \hookrightarrow & K \\ & {\scriptstyle j} \searrow & \\ & & K' \end{array}$$

"K est le plus petit corps contenant A et généralisant les lois + et × de A".

Division euclidienne :

$\forall a, b \in \mathbb{Z} \quad \exists q \in \mathbb{Z} \; \exists r \in \mathbb{N} \; / \; a = bq + r \qquad 0 \leq r < b$

Th | Tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$

Def | $a | b \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z}$

C'est une relation d'ordre partiel sur $\mathbb{N}$

$$a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z} \;(\delta \geq 0) \quad \delta = \Delta(a,b)$$
$$a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z} \;(\mu \geq 0) \quad \mu = \mathrm{ppcm}(a,b)$$

Théorème de Gauss

Th | $a | bc$ et $\delta(a,b)=1 \Rightarrow a | c$

$a, b \in \mathbb{N}$

Th | $\mu\delta = |ab|$ où $\mu = \mu(a,b)$ et $\delta = \delta(a,b)$

Corollaire : $\delta(a,b)=1 \Leftrightarrow \mu = ab$ $(a, b \in \mathbb{N})$

Nombres premiers

Def | $p \in \mathbb{N}$ est <u>premier</u> si $p\mathbb{Z}$ est <u>maximal</u> parmi les sous-groupes stricts (c.à.d $\neq \mathbb{Z}$)

Rappel : $(E, \leq)$ ensemble ordonné. $m$ est dit "él. maximal de E" si
$\forall e \in E \quad e \geq m \Rightarrow e = m$

Ainsi, $p$ premier ssi $a \neq 1$ et $a\mathbb{Z} \supset p\mathbb{Z} \Rightarrow a\mathbb{Z} = p\mathbb{Z}$

c.à.d, ssi $\begin{cases} a | p \\ a \neq 1 \end{cases} \Rightarrow a = p$ (définition habituelle)

Th | Tout nombre $(\neq 1) \in \mathbb{N}$ admet un diviseur premier

Un théorème équivalent est : "tout sous-groupe strict est contenu dans un sous-groupe maximal".

Par l'absurde : Si $G \subset \mathbb{Z}$, et $G$ n'est pas contenu dans un élément maximal. Donc $\exists G_1$ sous-groupe de $\mathbb{Z}$ tel que $G \subset G_1$.
$G_1 \neq$ s groupe maximal, sinon $G$ le serait.
Ainsi de suite : $G \subset G_1 \subset G_2 \subset \dots \subset G_k \subset \dots$ (suite strictement croissante)

<u>Lemme</u> : Toute suite croissante de sous-groupes de $\mathbb{Z}$ est stationnaire.

Preuve : Soit $(G_i)_{i \in \mathbb{N}}$ une suite croissante de sous-groupes de $\mathbb{Z}$. Alors $G_i \subset G_{i+1}$ $\forall i \in \mathbb{N}$.

$G = \bigcup_{i=1}^{\infty} G_i$ est un sous-groupe.

Posons $G_i = r_i \mathbb{Z}$ $\quad G = r\mathbb{Z}$

$r\mathbb{Z} = \bigcup G_i \Rightarrow \exists i \,/\, r \in G_i \Rightarrow r\mathbb{Z} \subset G_i$

$\Rightarrow G \subset G_i \Rightarrow G = G_i$

Ainsi, à partir de $i$, $G_i = G = r\mathbb{Z}$.

CQFD

Soit $\mathcal{P}$ l'ensemble des nombres premiers

Pro | $\mathcal{P}$ est infini (300 av JC)

Supposons que $\mathcal{P} = \{p_1, \dots, p_N\}$ et considérons $M = \left(\prod_{i=1}^{N} p_i\right) + 1$

$M$ n'est pas divisible par $p_i$ (car le reste de la division de $M$ par $p_i$ est 1).

Comme $M$ admet un diviseur premier (cf th. précédent) $p$, $p \notin \mathcal{P}$ ce qui est absurde.

Donc $\mathcal{P}$ est infini.

$\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, \dots\}$

<u>Factorisation unique en nombres premiers</u>

Résultat : $\forall p \in \mathcal{P}$ il existe une fonction $\nu_p : \mathbb{N}^* \longrightarrow \mathbb{N}$ telle que $n = 2^{\nu_2(n)} 3^{\nu_3(n)} \dots p^{\nu_p(n)} \dots$

où $p > n \Rightarrow \nu_p(n) = 0$

$$n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$$

(Existence et unicité)

↑ récurrence ↑ Th. de Gauss

1/ $\forall p \quad v_p(mn) = v_p(m) + v_p(n)$

En effet : $\begin{cases} m = p^{v_p(m)} . m' & \text{et } \Delta(p, m') = 1 \\ n = p^{v_p(n)} . n' & \text{et } \Delta(n', p) = 1 \end{cases}$

d'où $mn = p^{v_p(m)+v_p(n)} m'n' = p^{v_p(mn)} (m'n')$ et $\Delta(p, m'n') = 1$

2/ $\forall p \quad v_p(m+n) \geq \text{Inf}(v_p(m), v_p(n))$

Remarque : l'extension de cette décomposition à $\mathbb{Q}^*$ ($v_p : \mathbb{Q}^* \to \mathbb{Z}$) est faisable.

On peut définir $\mathbb{Q} \xrightarrow[| \, |_p]{} \mathbb{N}$ par $\begin{cases} |0|_p = 0 \\ q \neq 0, \quad |q|_p = p^{-v_p(q)} \end{cases}$

$| \, |_p$ vérifie : * $|qq'|_p = |q|_p |q'|_p$ (cf 1/)

* $|q + q'|_p \leq \text{Sup}(|q|_p, |q'|_p) \; (\leq |q|_p + |q'|_p)$

* $|q|_p = 0 \Rightarrow q = 0$

$| \, |_p$ est une "valeur absolue" sur $\mathbb{Q}$.

$\mathbb{Q}_p$ = corps p-adique = complexion de $\mathbb{Q}$ par la norme $| \, |_p$

$\mathbb{Q}_p = \{\text{ens. des suites de Cauchy p-adiques}\} / \sim$

Rappel : $\mathbb{Q} \hookrightarrow \mathbb{R}$ et $\mathbb{R} = \left\{ \begin{matrix} \text{ens. des suites de} \\ \text{Cauchy} \end{matrix} \right\} / \sim$

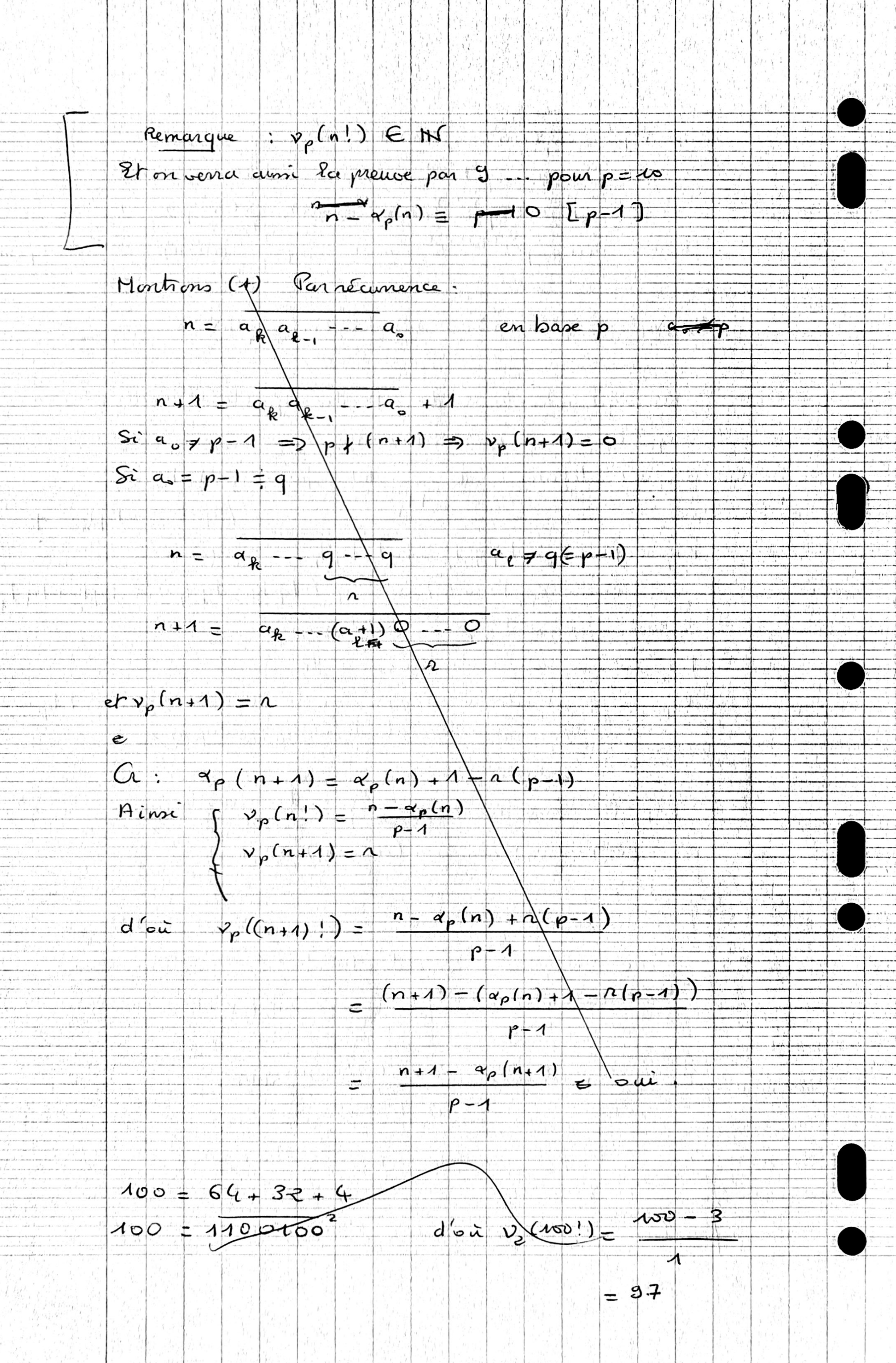
où $(u_n) \sim (v_n) \Leftrightarrow \lim_{+\infty} (u_n - v_n) = 0$

exercice : Nombre de zéros de 100 ! ?

$100! = 10^r . b$ où $10 \nmid b$ $\quad r = \text{Inf}(v_2(100!), v_5(100!))$

Pro $\Big| \quad v_p(n!) = \dfrac{n - \alpha_p(n)}{p-1} \qquad (1)$

où $\begin{cases} n = \sum_{i=0}^{\infty} a_i p^i & 0 \leq a_i < p \quad \text{(en base } p\text{)} \\ \alpha_p(n) = \sum_{i=0}^{\infty} a_i & \text{(en fait, somme finie)} \end{cases}$



Remarque : $\nu_p(n!) \in \mathbb{N}$

Et on verra ainsi la preuve par 9 ... pour $p=10$

$$n - \alpha_p(n) \equiv 0 \ [p-1]$$

Montrons (+) Par récurrence :

$n = \overline{a_k a_{k-1} \cdots a_0}$ en base $p$

$n+1 = \overline{a_k a_{k-1} \cdots a_0} + 1$

Si $a_0 \neq p-1 \Rightarrow p \nmid (n+1) \Rightarrow \nu_p(n+1) = 0$

Si $a_0 = p-1 \doteq q$

$n = \overline{a_k \cdots \underbrace{q \cdots q}_{r}}$ $\quad a_\ell \neq q (= p-1)$

$n+1 = \overline{a_k \cdots (a_\ell+1) \underbrace{0 \cdots 0}_{r}}$

et $\nu_p(n+1) = r$

Or : $\alpha_p(n+1) = \alpha_p(n) + 1 - r(p-1)$

Ainsi $\begin{cases} \nu_p(n!) = \dfrac{n-\alpha_p(n)}{p-1} \\ \nu_p(n+1) = r \end{cases}$

d'où $\nu_p((n+1)!) = \dfrac{n - \alpha_p(n) + r(p-1)}{p-1}$

$= \dfrac{(n+1) - (\alpha_p(n) + 1 - r(p-1))}{p-1}$

$= \dfrac{n+1 - \alpha_p(n+1)}{p-1}$ $\Leftarrow$ oui.

$100 = 64 + 32 + 4$

$100 = \overline{1100100}^2$ d'où $\nu_2(100!) = \dfrac{100-3}{1}$

$= 97$

Exercices

exercice 1 : Nombre de zéros de 100! ?

On a $100! = 10^r b$ où $10 \nmid b$ et $r = \text{Inf}(v_2(100!), v_5(100!))$

| Pro | $v_p(n!) = \dfrac{n - \alpha_p(n)}{p-1}$ |
|---|---|

(1)

où : $\begin{cases} n = \sum_{i=0}^{\infty} a_i p^i & 0 \le a_i < p \quad \text{(écriture en base } p) \\ \alpha_p(n) = \sum_{i=0}^{\infty} a_i & \text{(en fait, sommes finies)} \end{cases}$

Preuve : Montrons (1) par récurrence sur n

- vrai pour $n = 1$ $v_p(1) = 0$ $\forall p$ premier.
- vrai au rang $n$, ...

Notons $n = \overline{a_k a_{k-1} \cdots a_0}$ en base p

$n+1 = \overline{a_k a_{k-1} \cdots a_0} + 1$

De 2 choses l'une :

* Si $a_0 \neq p-1$, alors $p \nmid (n+1) \Rightarrow v_p(n+1) = 0$

d'où :

$$v_p((n+1)!) = v_p(n+1) + v_p(n!) = \frac{n - \alpha_p(n)}{p-1}$$

$$v_p((n+1)!) = \frac{(n+1) - \alpha_p(n+1)}{p-1} \quad \text{oui}$$

* Si $a_0 = p-1 \doteq q$, alors :

$$n = \overline{a_k a_{k-1} \cdots a_{r+1} \underbrace{q \cdots q}_{r \text{ fois}}} \quad \text{avec } a_i \neq q$$

$$n+1 = \overline{a_k \cdots (a_{r+1}+1) \underbrace{0 \cdots 0}_{r \text{ fois}}}$$

d'où $v_p(n+1) = r$

Ainsi $v_p((n+1)!) = v_p(n+1) + v_p(n!) = r + \frac{n - \alpha_p(n)}{p-1}$

$\alpha_p(n+1) = a_k + \dots + (a_{r+1}+1) = \alpha_p(n) - rq + 1$ , d'où :

$$v_p((n+1)!) = r + \frac{n - \alpha_p(n+1) - rq + 1}{p-1} = \frac{(n+1) - \alpha_p(n+1)}{p-1}$$

CQFD

exercice 2 : Avec les m notation qu'à l'ex. 1, montrer que $\frac{n - \alpha_p(n)}{p-1} \in \mathbb{N}$, lien avec la "preuve par neuf" ?

Solution : Nous avons :

$$n - \alpha_p(n) = \sum_{i=0}^{\infty} a_i (p^i - 1)$$

$\forall i \in \mathbb{N}^* \quad p^i - 1 = (p-1)(p^{i-1} + p^{i-2} + \dots + 1)$

d'où $n - \alpha_p(n) \equiv 0 \; [p-1]$

$$\boxed{n - \alpha_p(n) \equiv 0 \quad [p-1]}$$

Preuve par neuf : notons $\alpha(n) = \alpha_{10}(n)$ (syst. décimal)

a) Pour l'addition :

$\times \quad a + b = c \Rightarrow \alpha(a) + \alpha(b) \equiv \alpha(c) \quad [p-1]$

↑ c.à.d modulo 9

En effet : $\underbrace{a+b}_{} \equiv \alpha(a) + \alpha(b) \quad [p-1]$

$\parallel$
$c$
$\equiv$
$\alpha(c)$

b) Pour la multiplication

$\times \quad ab = c \Rightarrow \alpha(a)\,\alpha(b) \equiv \alpha(c) \quad [p-1]$

$$\begin{cases} a \equiv \alpha(a) & [p-1] \\ b \equiv \alpha(b) & [p-1] \end{cases} \Rightarrow ab \equiv \alpha(a)\alpha(b)$$

$$\Rightarrow \underbrace{c}_{\equiv \alpha(c)} \equiv \alpha(a)\,\alpha(b) \quad [p-1] \quad \text{oui}$$

Retour exercice 1

On a : $100 = 64 + 32 + 4 = \overline{1100100}^{2}$

d'où $v_2(100!) = \dfrac{100-3}{1} = 97$

d'autre part $v_5(100!) = \dfrac{100-4}{4} = 24$ car $100 = \overline{400}^{5}$

Le nbre de zéros dans 100! sera : 24

exercice 3 : Montrer que $v_p(C_{m+n}^{m}) = \dfrac{1}{p-1}(\alpha_p(m) + \alpha_p(n) - \alpha_p(m+n))$

On a $v\left(\dfrac{n_1}{n_2}\right) = v(n_1) - v(n_2)$ (si $\dfrac{n_1}{n_2} \in \mathbb{N}$)

donc :

$$v_p(C_{m+n}^{m}) = v_p((m+n)!) - v_p(m!\,n!)$$
$$= v_p((m+n)!) - v_p(m!) - v_p(n!)$$

cf. exo1 :

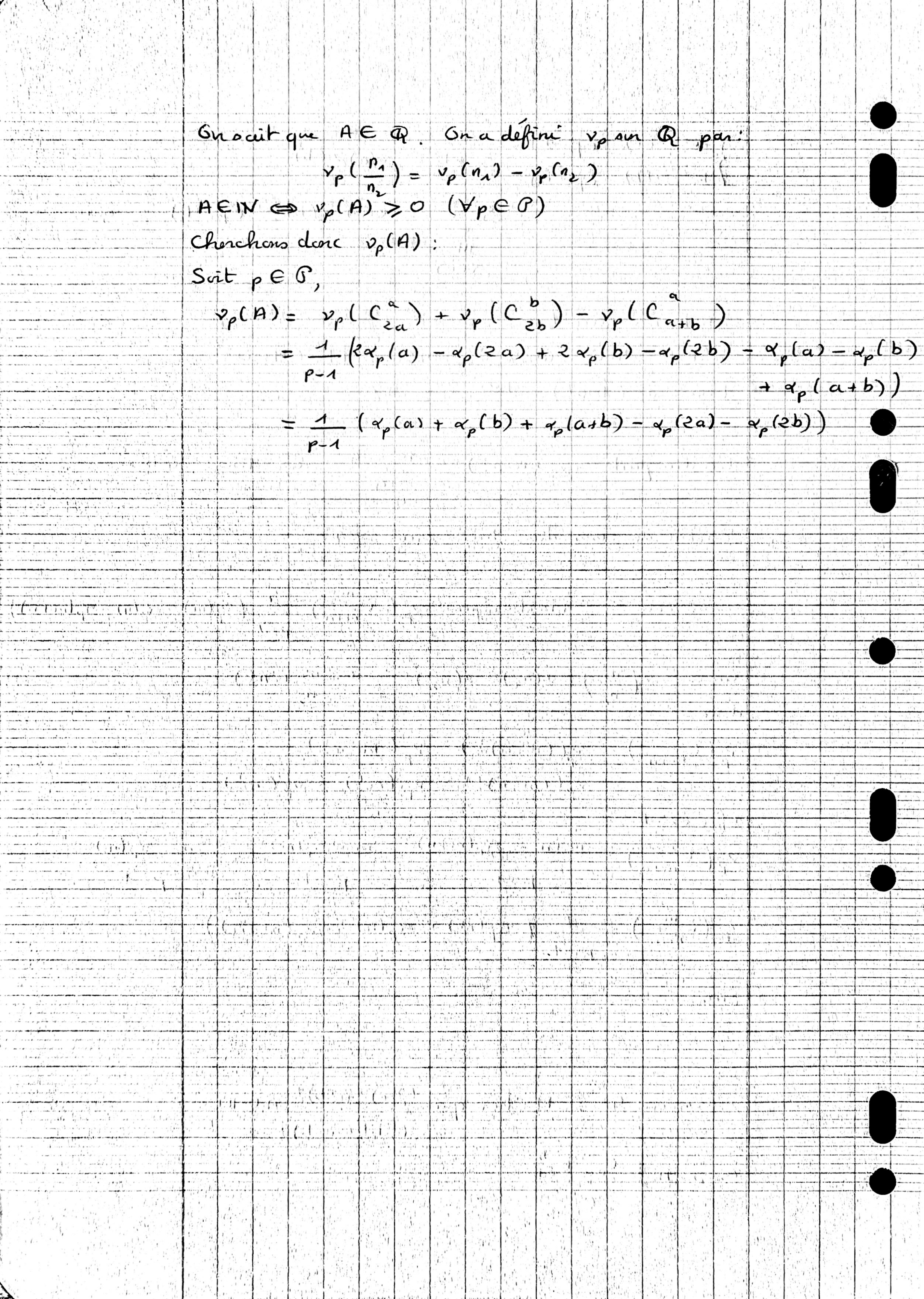
$$v_p(C_{m+n}^{m}) = \frac{m+n-\alpha_p(m+n)}{p-1} - \frac{m-\alpha_p(m)}{p-1} - \frac{n-\alpha_p(n)}{p-1}$$

$$v_p(C_{m+n}^{m}) = \frac{1}{p-1}\left(\alpha_p(m) + \alpha_p(n) - \alpha_p(m+n)\right)$$

oui.

exercice 4 : Montrer que $\dfrac{(2a)!\,(2b)!}{a!\,b!\,(a+b)!} = A \in \mathbb{N}$

On a $A = \dfrac{C_{2a}^{a}\, C_{2b}^{b}}{C_{a+b}^{a}}$



On sait que $A \in \mathbb{Q}$. On a défini $v_p$ sur $\mathbb{Q}$ par :

$$v_p\left(\frac{n_1}{n_2}\right) = v_p(n_1) - v_p(n_2)$$

$A \in \mathbb{N} \Leftrightarrow v_p(A) \geqslant 0 \quad (\forall p \in \mathcal{P})$

Cherchons donc $v_p(A)$ :

Soit $p \in \mathcal{P}$,

$$\begin{aligned} v_p(A) &= v_p(C_{2a}^{a}) + v_p(C_{2b}^{b}) - v_p(C_{a+b}^{a}) \\ &= \frac{1}{p-1}\Big(2\alpha_p(a) - \alpha_p(2a) + 2\alpha_p(b) - \alpha_p(2b) - \alpha_p(a) - \alpha_p(b) \\ &\qquad + \alpha_p(a+b)\Big) \\ &= \frac{1}{p-1}\left(\alpha_p(a) + \alpha_p(b) + \alpha_p(a+b) - \alpha_p(2a) - \alpha_p(2b)\right) \end{aligned}$$

Remarques diverses.

## 1°/ Systèmes de congruences

$m = \text{ppcm}(a,b)$

$\delta = \Delta(a,b)$

On a la suite exacte :

$$0 \to \mathbb{Z}/m\mathbb{Z} \xrightarrow{f} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \xrightarrow{g} \mathbb{Z}/\delta\mathbb{Z} \to 0$$

$$\dot{x}_m \longmapsto (\dot{x}_a, \dot{x}_b)$$

$$(\dot{y}_a, \dot{z}_b) \longmapsto (\dot{\overline{z-y}})_\delta$$

$f$ injective

$g$ surjective et $\text{Im} f = \text{Ker} g$.

Application :

Résoudre le système $\begin{cases} \dot{x}_a = \alpha \\ \dot{x}_b = \beta \end{cases}$

Ce système n'a de solution que si $(\alpha, \beta) \in \text{Im} f = \text{Ker} g$, c.à.d si $(\dot{\overline{\alpha - \beta}})_\delta = \dot{0}_\delta \iff \delta \mid (\beta - \alpha)$.

Dans ce cas, la solution $\dot{x}_m$ est unique (cf. $f$ injective) modulo le ppcm $(a,b) = m$.

## 2°/ Equation linéaire à 2 inconnue dans $\mathbb{Z}$.

On prendra garde de ne pas confondre l'étude du 1°/ et ce qui suit :

Résolution, dans $\mathbb{Z}^2$, de $ax + by = d$

- Si $\Delta(a,b) \nmid d$, pas de solutions.
- Si $\Delta(a,b) \mid d$, on est ramené à $a'x + b'y = d'$

où $\Delta(a', b') = 1$, que l'on résoud comme d'habitude. (voir une

leçon précédente)

3°/ Notation $GL(2, \mathbb{Z})$

$GL(2, \mathbb{Z})$ = ensemble des isomorphismes de $\mathbb{Z}^2 \to \mathbb{Z}^2$, en tant que groupes. On les représente matriciellement.

$$f = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \quad \text{où } a, b, c, d \in \mathbb{Z}.$$

Th | Soit M une matrices à coefficients entiers :

$$M \in GL(2, \mathbb{Z}) \iff \begin{cases} M \in GL(2, \mathbb{Q}) \\ \text{et} \\ \det M = \pm 1 \end{cases}$$

($\Rightarrow$) $M^{-1} \in GL(2, \mathbb{Z}) \Rightarrow MM^{-1} = I$ et $\underbrace{\det M}_{\in \mathbb{Z}} . \underbrace{\det M^{-1}}_{\in \mathbb{Z}} = 1$

d'où $\det M = \pm 1$

($\Leftarrow$) Soit $M \in GL(2, \mathbb{Q})$. Alors $M^{-1} = \frac{1}{\underbrace{\det M}_{= \pm 1}} \underbrace{{}^t\text{com} M}_{\text{coefficients dans } \mathbb{Z}}$.

donc $M^{-1}$ à coefficients entiers.

CQFD

Groupes abéliens libres de type fini (g a l t f)

Groupe abélien ⟺ $\mathbb{Z}$- module.

En effet, si $(E,+)$ est un groupe commutatif, alors :

1) $(E,+)$ = groupe com.

2) L'application externe $A \times E \to E$

$(\lambda, e) \mapsto \lambda e$ vérifie bien les 4 axioms

où $A = \mathbb{Z}$ et $\lambda e$ définit par $\begin{cases} 0e = e \\ \lambda e = e + (\lambda - 1)e \quad (\lambda > 0) \\ \lambda e = (-\lambda)(-e) \text{ si } \lambda < 0. \end{cases}$

1°/ Définitions

Def 1 : Un système libre de G est une famille $(g_i)_{i \in I}$ d'éléments de G tels que : $\sum_{\substack{i \in J \\ J \text{ fini}}} \lambda_i g_i = 0 \Rightarrow \lambda_i = 0 \quad \forall i \in J$

Def 2 : Un système générateur de G est une famille $(g_i)_{i \in I}$ d'él. de G tels que : $\forall g \in G \quad \exists J$ fini $\subset I$ / $\sum_{i \in J} \lambda_i g_i = g$

Remarque :

Considérons $\varphi : \mathbb{Z}^k \longrightarrow G$

$\lambda = (\lambda_1, \dots, \lambda_k) \longmapsto \varphi(\lambda) = \sum \lambda_i g_i$ (si I fini)

Alors :

$(g_1, \dots, g_k)$ libre ⟺ $\varphi$ injective

générateur ⟺ $\varphi$ surjective

base ⟺ $\varphi$ bijective.

Exo 1 : Dans $\mathbb{Z}/6\mathbb{Z}$, $(x)$ est un système lié car $6x = 0$.

$(x)$ générateur ⟺ $x = \dot{1}$ ou $\dot{5}$

Exo 2 : $G = (\mathbb{Q}, +)$

$(r)$ libre si $r \neq 0$, puisque $xr = 0 \Rightarrow x = 0$

Mais le système $(r, s)$ est lié pour tout $(r,s) \in \mathbb{Q}$. Cela voudrait-il dire que $\dim \mathbb{Q} = 1$ ? Non ! Car il n'existe pas de systèmes généra-

termes finis ! En effet, pour $(r_1, \dots, r_k)$ donnés, posons $r_i = \frac{p_i}{q_i}$
et considérons $\sum_{i=1}^{k} \lambda_i \frac{p_i}{q_i} = \frac{a}{\prod q_i}$

$\exists p \in \mathcal{P}$ tel que $p \nmid q_1 \cdots q_k \Rightarrow \frac{a}{\prod q_i} \neq \frac{1}{p}$

Remarquons bien que, si $G = \mathbb{Q}$, alors $G$ ne possède pas de base.
Il n'y a alors aucun espoir de démontrer un équivalent du th. de la base incomplète dans $G$.

Def | Un groupe abélien $G$ est dit
1) "libre" s'il possède une base.
2) "de type fini" s'il possède un système de générateurs finis.

On notera "galtf" un groupe abélien libre de type fini.
ex : $\mathbb{Z}$, $\mathbb{Z}^2$ sont des galtf ; $\mathbb{Z}[X]$ ou $\mathbb{R}[X]$ sont libres mais non de type fini.

Mise en garde : Une partie libre maximale n'est pas forcément une base. Ainsi, dans $\mathbb{Z}$, $\{2\}$ est partie libre maximale et pourtant $\langle\{2\}\rangle = 2\mathbb{Z} \neq \mathbb{Z}$.

Pro | Tout g.a.l.t.f est isomorphe à $\mathbb{Z}^n$

Soit $G$ un galtf. Alors $G$ possède un syst. gén. fini, et une base.
On montre qu'alors $G$ possède une base finie $(a_1, \dots, a_n)$. On considère enfin l'application $\varphi : \mathbb{Z}^n \to G : (\lambda_1, \dots, \lambda_n) \mapsto \sum_{i=1}^{n} \lambda_i a_i$.

Théorème Fondamental

Th | Tout sous-groupe $H$ d'un g.a.l.t.f $G$ ($G \simeq \mathbb{Z}^n$) est un galtf, et $H \simeq \mathbb{Z}^m$ où $m \leq n$

Remarque : $G$ de type fini $\Leftrightarrow$ $G \simeq \mathbb{Z}^n/_H$ ($H$ sous-groupe de $\mathbb{Z}^n$)

$(g_1, \dots, g_k)$ syst. générateur $\Rightarrow \varphi : \mathbb{Z}^n \xrightarrow{surj} G$

$$\begin{array}{ccc} \mathbb{Z}^n & \xrightarrow{surj} & G \\ \downarrow & \nearrow \simeq & \\ \mathbb{Z}^n/_{\ker\varphi} & & \end{array}$$

**lemme** : Soit la suite exacte

$$0 \longrightarrow \mathbb{Z}^r \xrightarrow{f} G \xrightarrow{g} \mathbb{Z}^s \longrightarrow 0$$

(c.à.d : $f$ injective, $g$ surjective et $\ker g = \operatorname{Im} f$ )

Alors $G \simeq \mathbb{Z}^{r+s}$.

En effet :

On a $\mathbb{Z}^{r+s} \simeq \mathbb{Z}^r \times \mathbb{Z}^s$.

$G \underset{j}{\overset{g}{\rightleftarrows}} \mathbb{Z}^s$ $\qquad \exists j \,/\, g \circ j = Id$ où $j \in Hom(\mathbb{Z}^s, G)$

$a_1, \dots, a_s \in G$
$$\begin{cases} g(a_1) = (1, 0, \dots 0) \\ \text{----} \\ g(a_s) = (0, \dots, 1) \end{cases} \quad (*)$$

Se donner $j$ revient à se donner $s$ éléments $a_1, \dots, a_s$ tels que $(*)$ ait lieu. C'est possible car $g$ est surjective.

Cela étant :

$$\chi : \mathbb{Z}^r \times \mathbb{Z}^s \longrightarrow G$$
$$(\lambda, \mu) \longmapsto f(\lambda) + j(\mu)$$

où $\lambda = (\lambda_1, \dots, \lambda_r)$
$\mu = (\mu_1, \dots, \mu_s)$

On a : $f : \mathbb{Z}^r \to G$, donc $f$ défini par $(b_1, \dots, b_r) \in G^r$ :

$$f(\lambda) = \sum_{i=1}^{r} \lambda_i b_i$$

Ainsi :

$$\chi(\lambda, \mu) = \sum_{i=1}^{r} \lambda_i b_i + \sum_{i=1}^{s} \mu_i a_i$$

Montrons que $\chi$ est bijective (c'est un homomorphisme !)

* $\chi$ injective.

$$f(\lambda) + j(\mu) = 0 \Rightarrow \underbrace{g \circ f(\lambda)}_{0} + \mu = 0 \Rightarrow \mu = 0$$

(car la suite est exacte $\operatorname{Im} f = \ker g$)

Donc $f(\lambda)=0 \Rightarrow \lambda = 0 \in \mathbb{Z}^n$ (car $f$ injective)

$*$ $\chi$ surjective. Soit $x \in G$

$\exists ? \lambda, \mu$ / $x = f(\lambda)+j(\mu) \Rightarrow g(x) = \underbrace{g\circ f(\lambda)}_{=0} + \underbrace{g\circ j}_{Id}(\mu)$

donc $g(x) = \mu$

et $f(\lambda) = x - j(g(x))$

On cherche $\lambda$. Ce $\lambda$ n'existera que si $x - j\circ g(x) \in \mathrm{Im} f = \mathrm{Ker}\, g$,

c.à.d si $g(x - j\circ g(x)) = 0$

$g(x) - g(x) = 0$ oui.

Donc $\exists \lambda \in \mathbb{Z}^n$ tel que $f(\lambda) = x - j(g(x))$.

$\chi$ est bien surjective.

Démonstration du théorème : récurrence sur $n$

a) $n=1$, ~~le lemme nous donne~~ :

$G \simeq \mathbb{Z}$ Soit $\varphi$ l'isomorphisme.

$H \subset G \Leftrightarrow \varphi(H) \subset \mathbb{Z} \Leftrightarrow \exists r \in \mathbb{N} / \varphi(H) = r\mathbb{Z}$

d'où $H = \{ x \in G / \exists k \in \mathbb{Z} \quad x = \varphi^{-1}(r)\varphi^{-1}(k)\}$

ou, ce qui revient au même : $H = \varphi^{-1}(r).G$

b) hypothèse vraie $\forall p \leq n$. Est-elle vraie au rang $n+1$?

Soit $H \subset \mathbb{Z}^{n+1}$. On a l'homomorphisme surjectif :

$$\mathbb{Z}^{n+1} \xrightarrow{p} \mathbb{Z}$$

$$(x_1, \dots, x_{n+1}) \longmapsto x_{n+1}$$

dont le noyau est isomorphe à $\mathbb{Z}^n$.

D'où la suite exacte :

$$0 \longrightarrow \mathbb{Z}^n \xrightarrow{f} \mathbb{Z}^{n+1} \underset{\xleftarrow{\ \rho\ }}{\twoheadrightarrow} \mathbb{Z} \longrightarrow 0$$

$$(\lambda_1, \dots, \lambda_n) \quad (\lambda_1, \dots, \lambda_n, 0)$$

$$0 \longrightarrow \mathbb{Z}^n \xhookrightarrow{f} \mathbb{Z}^{n+1} \xrightarrow{p} \mathbb{Z} \longrightarrow 0 \qquad (1)$$

$$\cup$$

$$0 \longrightarrow H\cap\mathbb{Z}^n \hookrightarrow H \xrightarrow[p|_H]{} p(H) \longrightarrow 0 \qquad (2)$$

où $H\cap\mathbb{Z}^n = \{(\lambda_1, \dots, \lambda_n)$ telles que $(\lambda_1, \dots, \lambda_n, 0) \in H\}$ (abus d'écriture)

(2) est aussi une suite exacte.

$H\cap\mathbb{Z}^n$ = sous-groupe de $\mathbb{Z}^n$ $\Rightarrow$ il est libre de type fini.

Donc $H\cap\mathbb{Z}^n \simeq \mathbb{Z}^r$ $(r \leq n)$

De même, $p(H) \simeq \mathbb{Z}^s$ où $s \leq 1$

On applique le lemme :

$$H \simeq \mathbb{Z}^{r+s} \quad \text{où} \quad r+s \leq n+1$$

CQFD

2% Présentation de G

Soit G un galtf. Il existe un homomorphisme surjectif $\varphi$

$$\varphi : \mathbb{Z}^m \twoheadrightarrow G$$

$$\cup \quad \uparrow f$$

$$\text{Ker}\,\varphi \simeq \mathbb{Z}^n \quad (n \leq m)$$

et alors $G \simeq \mathbb{Z}^m/\text{Im}\, f$ où $f$ = isomorphisme de $\text{Ker}\,\varphi$ vers $\mathbb{Z}^m$.

On peut faire le diagramme :

$$\mathbb{Z}^n \xrightarrow{f} \mathbb{Z}^m \overset{\varphi}{\twoheadrightarrow} G \longrightarrow 0$$

$$\wr\!\wr \qquad \cup$$

$$\text{Ker}\,\varphi$$

(suite exacte.)

C'est une "présentation de G".

On constate que l'on a bien : $G \simeq \mathbb{Z}^m/_{\text{Ker}\,\varphi}$ et $\text{Ker}\,\varphi = \text{Im}\, f$.

Exemple 1 :

$$\mathbb{Z} \longrightarrow \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/a\mathbb{Z} \qquad (a>0)$$
$$\lambda \longmapsto \lambda a ; 1 \longmapsto \dot{1}$$

Exemple 2 :

Chercher $\mathbb{Z}^2/\mathrm{Im}\, s$ où $s : \mathbb{Z} \to \mathbb{Z}^2$
$\lambda \mapsto (\lambda, \lambda)$

On a la suite exacte :

$$\mathbb{Z} \xrightarrow{s} \mathbb{Z}^2 \xrightarrow{\varphi} \mathbb{Z} \longrightarrow 0$$
$$\lambda \longmapsto (\lambda, \lambda)$$
$$(\lambda, \mu) \longmapsto \lambda - \mu$$

d'où $\mathbb{Z}^2/_{\mathrm{Ker}\,\varphi} = \mathbb{Z}^2/_{\mathrm{Im}\, s} \simeq \mathbb{Z}$.

Exemple 3 :

Si $s : \mathbb{Z} \to \mathbb{Z}^2$, montrer que $\mathbb{Z}^2/_{\mathrm{Im}\, s} \simeq \mathbb{Z}$
$\lambda \mapsto (2\lambda, -\lambda)$

On a la suite exacte

$$\mathbb{Z} \xrightarrow{s} \mathbb{Z}^2 \xrightarrow{\varphi} \mathbb{Z} \to 0$$
$$\lambda \mapsto (2\lambda, -\lambda)$$
$$(\lambda, \mu) \longmapsto 2\lambda + \mu$$

d'où $\mathbb{Z}^2/_{\mathrm{Im}\, s} \simeq \mathbb{Z}$

III Matrices à coefficients entiers.

## 1°/ Rappels sur les matrices à coefficients dans K

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \alpha\uparrow & & \uparrow\beta \\ K^n & \xrightarrow{M} & K^m \\ \nearrow T & & \nearrow S \\ K^n & \xrightarrow[M']{} & K^m \end{array}$$

$f \in \mathcal{L}(E,F)$

$M = \beta^{-1} f \alpha$ = matrice de $f$ dans les bases $\alpha, \beta$

$M' = S^{-1}MT$ ($\Leftrightarrow$ $M'$ équivalente à $M$)

où $S \in GL(m,K)$ et $T \in GL(n,K)$

Deux matrices sont $\sim$ si elles représentent la m̂ application dans des bases diff. à la source et au but.

On peut parler d'action de groupe :

$$GL(n) \times GL(m) \text{ opère sur } M(m,n,K)$$
$$(M,S)T = S^{-1}MT$$

<u>Pro</u> : Sur un corps K, deux mat. sont équivalentes ssi elles ont m̂ rang (Et dans un anneau ?)

Notion <u>complètement</u> différente de celle de matrice semblable !

<u>Matrices semblables.</u>

$$\begin{array}{ccc} E & \xrightarrow{u} & E \\ \alpha\uparrow & & \uparrow\beta=\boxed{\alpha} \\ K^n & \xrightarrow{M} & K^n \\ S\nearrow & & \nearrow\boxed{S} \\ K^n & \xrightarrow[M']{} & K^n \end{array}$$

$u \in \mathcal{L}(E,E)$

$M' = S^{-1}MS$ (relation plus fine que l'autre)

$GL(n)$ opère à droite sur $M(n,K)$ : $MS = S^{-1}MS$

C'est alors que l'on parle de "triangularisation", de "matrices de Jordan".

Le problème de la similitude des matrices est très difficile. Aussi nous poserons nous le problème de l'équivalence des matrices.

## 2/ Matrices à coefficients entiers

**Théorème fondamental** : Toute matrice $m \times n$ à coefficients dans $\mathbb{Z}$ est équivalente à une matrice de la forme

$$\begin{pmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & \ddots & \\ 0 & & & d_k \end{pmatrix} \qquad \begin{array}{l} k = \inf(m,n) \\ d_i \in \mathbb{N} \end{array}$$

et $d_1 | d_2$ ; $d_2 | d_3$ ; ... ; $d_{k-1} | d_k$

Ce sont les diviseurs élémentaires de la matrices. Ils ne dépendent que de $M$.

Preuve : Le problème : trouver $S$ et $T$ inversibles telles que

$$M' = TMS = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_k \end{pmatrix}$$

Opérations élémentaires sur les matrices :

Sur les lignes : 1) Permuter 2 lignes $i, j$.

2) changer de signe une ligne

3) ajouter, à une ligne, un multiple entier d'une autre [ligne]

(même chose pour les colonnes)

1) = chgt de base. C'est permuter $\varepsilon_i$ et $\varepsilon_j$

2) = chgt de base. C'est remplacer le vecteur de base $\varepsilon_i$ par $(-\varepsilon_i)$

3) = "

$$\begin{pmatrix} a & a' \\ b & b' \\ c & c' \end{pmatrix} \begin{matrix} \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \end{matrix} \quad \leadsto \quad \begin{pmatrix} -a & -a' \\ b & b' \\ c & c' \end{pmatrix} \begin{matrix} -\varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \end{matrix}$$

(colonnes : $f(e_1)$, $f(e_2)$)

• **Th** : Toute opération élémentaire sur les lignes (resp. colonnes) correspondent à un changement de base dans le groupe d'arrivée (resp. de départ) c.à.d à la multiplication de la matrice à gauche (resp. à droite) par une matrice inversible.

• **Remarque** : Cette matrice inversible s'obtient en effectuant l'opération en question sur les lignes (resp. colonnes) de la matrice identité.

**Exemples:**

* Si $M = \begin{pmatrix} a & a' \\ b & b' \\ c & c' \end{pmatrix}$, changer de signe la première ligne.

$(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ changée en $(-\varepsilon_1, \varepsilon_2, \varepsilon_3)$ et : $S = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & a' \\ b & b' \\ c & c' \end{pmatrix} = \begin{pmatrix} -a & -a' \\ b & b' \\ c & c' \end{pmatrix}$$

* Si $M = \begin{pmatrix} a & a' \\ b & b' \\ c & c' \end{pmatrix}$, faire 1^e ligne + $\lambda$(2^e ligne)

$$\omega(M) = \begin{pmatrix} a+\lambda b & a'+\lambda b' \\ b & b' \\ c & c' \end{pmatrix} = SM$$ (On sait qu'il existe S inversible.)

Alors $\omega(I) = S = \begin{pmatrix} 1 & \lambda & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ où $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

d'où :

$$\begin{pmatrix} 1 & \lambda & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & a' \\ b & b' \\ c & c' \end{pmatrix} = \begin{pmatrix} a+\lambda b & a'+\lambda b' \\ b & b' \\ c & c' \end{pmatrix}$$

Pour montrer le th. fondamental, nous allons prouver que pour toutes matrices, il existe une suite d'opérations élémentaires sur les lignes et les colonnes, qui la met sous la forme

$$\begin{pmatrix} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_k & \end{pmatrix}$$

On démontre ce résultat par récurrence :

Définissons $d_1$ = plus petit coefficient positif de toutes les matrices déduites de M par opérations élémentaires.

Au bout d'un certain nombre d'étapes, je peux obtenir la matrice :

$$\begin{matrix} i' \cdots \\ i \cdots \end{matrix} \begin{pmatrix} & a & \\ & | & \\ \text{---} & d_1 & \text{---} \\ & | & \end{pmatrix}$$

Soit $a > 0$ (sinon, on change le signe de la colonne), $a \in$ colonne de $d_1$.

On a : $a = q d_1 + r \qquad 0 \leq r < d_1$

L'opération « $i'$ ligne $- q$ ($i$ ligne) » donne une matrice, équivalente par op. élémentaires, possédant le coefficient $r < d_1$, ce qui est absurde car $d_1 = \text{Inf}$(de ces coefficients).

Donc $r = 0$ (*)

On obtient :

$$\begin{pmatrix} & 0 & \\ & \vdots & \\ 0 \cdots & d_1 & \cdots 0 \\ & \vdots & \\ & 0 & \end{pmatrix}$$

d'où :

$$\begin{pmatrix} d_1 & 0 \cdots 0 \\ 0 & d_2 \cdots \\ \vdots & \vdots \quad N \\ 0 & \end{pmatrix}$$

Et $d_1$ divise tous les éléments de la matrice N, car, par opérations élémentaires :

$$\begin{pmatrix} d_1 & d_1 \cdots 0 & \\ 0 & d_2 & 0 \\ \vdots & \vdots \quad N & \\ 0 & & \end{pmatrix} \Rightarrow (*) \quad d_1 | d_2$$

CQFD

<u>Remarque</u> : On verra que $d_1 = \text{pgcd}(a_{ij})$ et que les $d_i$ ne dépendent que de $M$, au 4°/.

3°/ <u>Application</u> : <u>Résolution en nbres entiers de systèmes linéaires à coefficients entiers.</u>

$$\begin{array}{ccccc} X & \mathbb{Z}^n & \xrightarrow{M} & \mathbb{Z}^m & Y \\ & S \downarrow & & \downarrow T & \\ X' & \mathbb{Z}^n & \xrightarrow[D]{} & \mathbb{Z}^m & Y' \end{array}$$

Il existe un changement de base $S$ et $T$ tels que :

$$\begin{pmatrix} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_k & \end{pmatrix} = D = T^{-1} M S$$

$$\boxed{\begin{cases} X = SX' \\ Y = TY' \end{cases}}$$

Comment calculer $S, T, D$ sans se fatiguer ?

Soit $\omega'$ la succession des opérations sur les colonnes effectuées pour passer de $M$ à $D$ : $\begin{cases} \omega'(M) = MS \\ \omega'(I_n) = S \end{cases}$

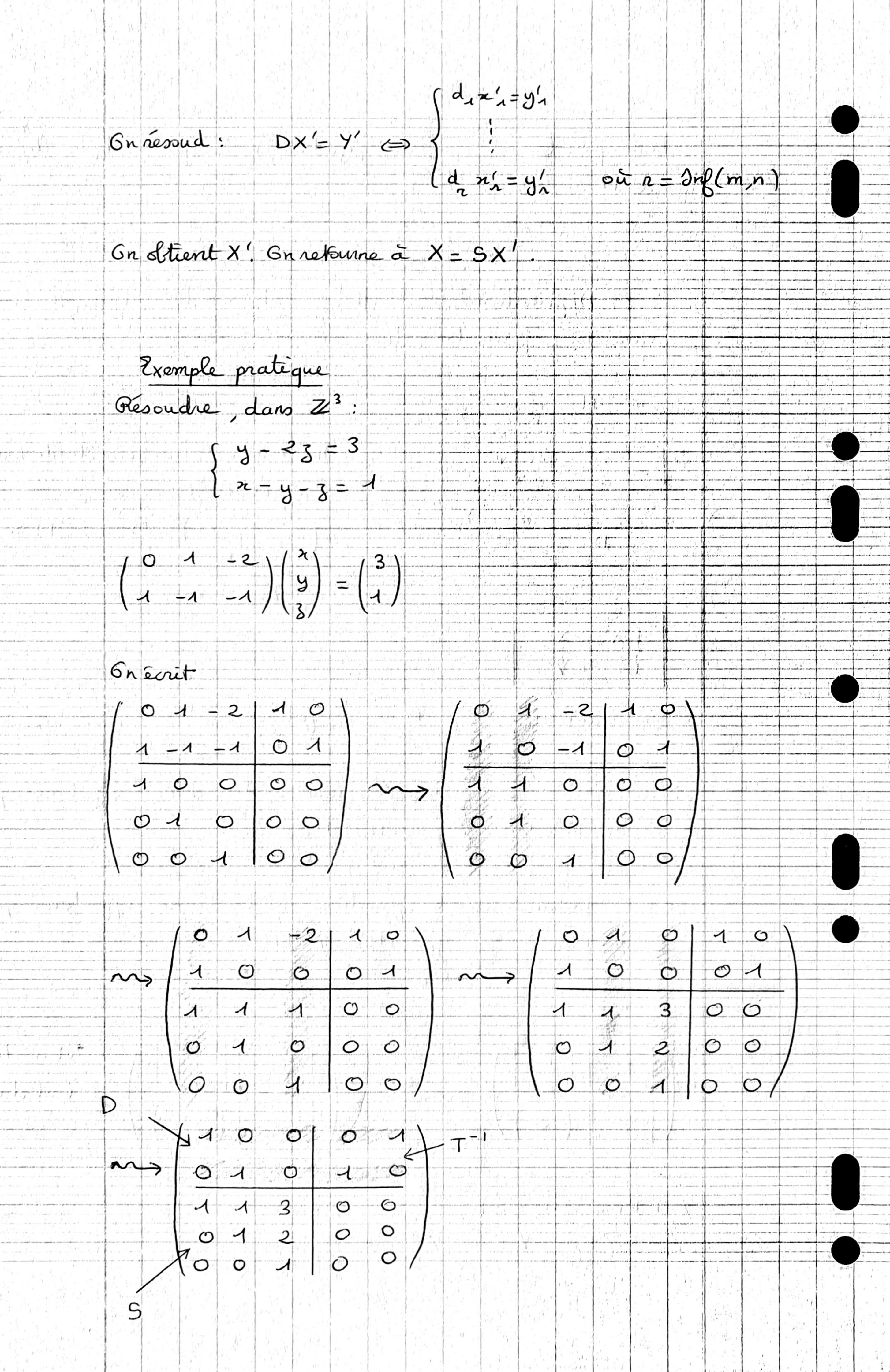
Soit $\omega''$ la succession des opérations sur les lignes effectuées pour passer de $M$ à $D$ : $\begin{cases} \omega''(M) = T^{-1}M \\ \omega''(I_m) = T^{-1} \end{cases}$

$$m\left\{\begin{pmatrix} \overbrace{\boxed{M}}^{n} & \boxed{I_m} \\ \boxed{I_n} & (0) \end{pmatrix}\right. \xrightarrow[\omega'']{\omega'} \begin{pmatrix} \boxed{D} & \boxed{T^{-1}} \\ \boxed{S} & (0) \end{pmatrix}$$

et on obtient <u>tout d'un coup</u> !

$Y$ est donné. On écrit :

$$Y' = T^{-1} Y$$



On résoud : $DX' = Y' \iff \begin{cases} d_1 x'_1 = y'_1 \\ \vdots \\ d_r x'_r = y'_r \end{cases}$ où $r = \mathrm{Inf}(m,n)$

On obtient $X'$. On retourne à $X = SX'$.

## Exemple pratique

Résoudre, dans $\mathbb{Z}^3$ :

$$\begin{cases} y - 2z = 3 \\ x - y - z = 1 \end{cases}$$

$$\begin{pmatrix} 0 & 1 & -2 \\ 1 & -1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$$

On écrit

$$\left(\begin{array}{ccc|cc} 0 & 1 & -2 & 1 & 0 \\ 1 & -1 & -1 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|cc} 0 & 1 & -2 & 1 & 0 \\ 1 & 0 & -1 & 0 & 1 \\ \hline 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right)$$

$$\rightsquigarrow \left(\begin{array}{ccc|cc} 0 & 1 & -2 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ \hline 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|cc} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ \hline 1 & 1 & 3 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right)$$

$$\rightsquigarrow \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ \hline 1 & 1 & 3 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right)$$

D

$T^{-1}$

S

$$Y' = T^{-1}\begin{pmatrix}3\\1\end{pmatrix} = \begin{pmatrix}1\\3\end{pmatrix} = DX'$$

$X' = \begin{pmatrix}x'\\y'\\z'\end{pmatrix}$  $DX' = \begin{pmatrix}1\\3\end{pmatrix} \Leftrightarrow \begin{cases} x' = 1 \\ y' = 3 \end{cases} \quad \forall z'$

d'où $X = \begin{pmatrix}x\\y\\z\end{pmatrix}$ solution ssi $X = SX' = \begin{pmatrix}1&1&3\\0&1&2\\0&0&1\end{pmatrix}\begin{pmatrix}1\\3\\z'\end{pmatrix}$

La solution générale est : $X = \begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}4+3z'\\3+2z'\\z'\end{pmatrix} \quad \forall z' \in \mathbb{Z}$

## 4°/ Les $d_i$ ne dépendent que de la matrice M

Remarque : Les 2 relations d'équivalences suivantes sont, à priori, différentes :

$$\begin{cases} M \sim M' \Leftrightarrow \exists S, T \text{ inversibles } / \ M' = TMS \\ M \underset{opel}{\sim} M' \Leftrightarrow \exists\ \omega \text{ opération élémentaire } / \ M' = \omega(M) \end{cases}$$

$\Updownarrow$

$\exists S, T$, produits de matrices élémentaires / $M' = TMS$

En fait, ce sont les $\underline{\underline{\hat{m}}}$ relations :

Th : Toute matrice inversible est produit de matrices élémentaires de la forme $\begin{pmatrix}1 & & 0\\ & -1 & \\ 0 & & 1\end{pmatrix}$, $\begin{pmatrix}1 & & 0\\ & \boxed{\begin{smallmatrix}0&1\\1&0\end{smallmatrix}} & \\ 0 & & 1\end{pmatrix}$ ou $\begin{pmatrix}1 & & \lambda\\ & \ddots & \\ & & 1\end{pmatrix}$ $(\sigma^{\lambda})$

$j^{e}$ colonne ; permuté 2 colonnes.

En effet, $M \in GL(n, \mathbb{Z})$ $\exists S, T$ produits de matrices élémentaires telles que : $D = TMS$

et $D^{-1} = S^{-1}M^{-1}T^{-1}$

Or $D \in GL(n, \mathbb{Z}) \Rightarrow \det D = \pm 1 = d_1 \cdots d_n \Rightarrow d_i = \pm 1 \quad i \in [1, n]$

donc $TMS = I$ (par une opération élémentaire en plus, s'il le faut!)

$\Downarrow$

$M = T^{-1}S^{-1}$

Ce sont des matrices élémentaires

oui.

(Notons, en passant, que les matrices du type (T) engendrent $GL(n, \mathbb{Z})$)

Th

Soit $M = (a_{ij})$ équivalente à $D = (d_1, \dots, d_n)$

Alors $d_1 = \text{pgcd}(a_{ij})$.

Plus généralement,

$$d_1 \dots d_k = \text{pgcd (mineurs d'ordre } k \text{ de } M)$$

Remarque : les $d_i$ ne dépendent donc que de la matrice

En fait, ils ne dépendent que de l'homomorphisme.

exo : Montrer que deux matrices $M$ et $M'$ sont $\sim$ ssi elles ont m̂ diviseurs élémentaires.

Preuve :

Le pgcd des mineurs d'ordre $k$ est invariant par opérations élémentaires (car $\text{pgcd}(a, b) = \text{pgcd}(a + \lambda b, b)$ )

$$k \updownarrow \begin{pmatrix} \boxed{\begin{matrix} a_1+\lambda b_1 & \dots & b_1 \\ \vdots & \ddots & \\ a_k+\lambda b_k & \dots & b_k \end{matrix}} & \\ & \end{pmatrix} \quad \text{et pgcd} \begin{pmatrix} a_1+\lambda b_1 & \dots & b_1 \\ \vdots & \ddots & \\ a_k+\lambda b_k & \dots & b_k \end{pmatrix}$$

$\overleftrightarrow{k}$

$$= \text{pgcd} \begin{pmatrix} a_1 & \dots & b_1 \\ \vdots & \ddots & \vdots \\ a_k & \dots & b_k \end{pmatrix}$$

oui.

# Application aux groupes abéliens libres de type fini

## 1% Rang d'un galtf. Propriété.

Pro 1 | Deux bases d'un même g.a.l.t.f ont même cardinal, appelé rang du groupe.

Soit $G$ un galtf, montrons que $G \simeq \mathbb{Z}^r$ et $G \simeq \mathbb{Z}^s \Rightarrow r = s$

Soit l'isomorphisme $\varphi : \mathbb{Z}^r \to \mathbb{Z}^s$. $\varphi$ a pour matrice $s \times r$ :

$$\text{mat}(\varphi) = \underbrace{\begin{pmatrix} \times & \times & \cdots \\ \vdots & \times & \\ \times & \cdots & \times \end{pmatrix}}_{r} \Big\updownarrow s$$

et d'après ce qui précède : $\text{mat}(\varphi) \sim \begin{pmatrix} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_t & \end{pmatrix}$

où $t = \text{Inf}(r, s)$

Si $r > s$, il y a au moins une colonne nulle, et donc $\varphi$ n'est pas injective. Si $r < s$, il y a au moins une ligne nulle, et donc $\varphi$ n'est pas surjective. Donc $r = s$. CQFD

Pro 2 | Si 2 galtf sont isomorphes, alors ils ont même rang.

$$\begin{array}{ccc} G & \xrightarrow{\sim} & G' \\ s\downarrow & & \downarrow s \\ \mathbb{Z}^r & & \mathbb{Z}^s \end{array}$$

donc $\mathbb{Z}^r \simeq \mathbb{Z}^s \Rightarrow r = s \Leftrightarrow G$ et $G'$ m̂ rang.

Pro 3 | $G$ = galtf de rang $m$ ($G \simeq \mathbb{Z}^m$)
$H$ = sous-groupe de $G$.
Il existe une base $(e_1, \dots, e_n)$ de $G$ et $d_1, \dots, d_k \in \mathbb{Z}^*$ $(d_i | d_{i+1})$ tels que $(d_1 e_1, \dots, d_k e_k)$ soit une base de $H$.

Preuve :

Puisque G est un galtf, $\exists \Psi$ isom / $G \xrightarrow{\Psi} \mathbb{Z}^m$. Or H est un sous-groupe de G, c'est aussi un galtf d'où :

$\exists \varphi$ isom / $H \xrightarrow{\varphi} \mathbb{Z}^n$ et $rg(H) \leq rg(G) \Leftrightarrow n \leq m$

$$\begin{array}{ccc} H & \overset{i}{\hookrightarrow} & G \\ \varphi \wr \downarrow & & \downarrow \wr \Psi \\ \mathbb{Z}^n & \xrightarrow{\theta} & \mathbb{Z}^m \end{array}$$

$\theta = \Psi \circ i \circ \varphi^{-1}$ morphisme injectif de $\mathbb{Z}^n$ vers $\mathbb{Z}^m$

D'après le th. fondamental, $mat(\theta) \sim \begin{pmatrix} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_k & \end{pmatrix}$ où $d_i | d_{i+1}$

c.à.d :

$\exists$ base $(\xi_1, \dots, \xi_n)$ de $\mathbb{Z}^n$

$\exists$ base $(\varepsilon_1, \dots, \varepsilon_m)$ de $\mathbb{Z}^m$

où $\begin{cases} \theta(\xi_i) = d_i \varepsilon_i & i \leq k \quad (k = Inf(n,m)) \\ \theta(\xi_i) = 0 & si\ i > k \end{cases}$

Mais $\theta$ étant injectif, $\theta(\xi_i) = 0$ pour $i > k$ est impossible, d'où $k = n$.

Revenons, maintenant, à G et à H.

Soit $e_i = \Psi^{-1}(\varepsilon_i) \quad \forall i \in [1, m]$

$\Psi$ isom $\Rightarrow (e_1, \dots, e_m)$ = base de G

Qu'est-ce que $\varphi^{-1}(\xi_i)$ ?

On a : $\quad \Psi[i(\varphi^{-1}(\xi_i))] = \theta(\xi_i) = d_i \varepsilon_i = \Psi(d_i e_i)$

d'où $\quad \Psi(\varphi^{-1}(\xi_i)) = \Psi(d_i e_i)$

$$\Updownarrow$$

$$\varphi^{-1}(\xi_i) = d_i e_i$$

Or $\varphi^{-1}(\xi_i)$ est une base de H. Donc $(d_1 e_1, \dots, d_n e_n)$ est une base de H. CQFD

## 2°/ Théorème fondamental des gatf

**Th** Soit $G$ un gatf. Il existe $d_1, \dots, d_k \in \mathbb{N}^*$ $d_i | d_{i+1}$ et un nombre $r \in \mathbb{N}$ tels que :

$$G \simeq \prod_{1 \leq i \leq k} \mathbb{Z}/_{d_i\mathbb{Z}} \times \mathbb{Z}^r$$

et cette décomposition est unique.

Démonstration :

• existence

$G$ gatf $\Rightarrow \exists\ \mathbb{Z}^m \xrightarrow{f} G$ surjectif

$\operatorname{Ker} f$ = sous-groupe de $\mathbb{Z}^m$, donc $G \simeq \mathbb{Z}^m/_{\operatorname{Ker} f}$ et, d'après la Pro 3 :

$\exists$ base $(e_1, \dots, e_m)$ de $\mathbb{Z}^m$ et des nombres $d_1, \dots, d_k \neq 0$ $(d_i | d_{i+1})$ tels que $(d_1 e_1, \dots, d_k e_k)$ soit une base de $\operatorname{Ker} f$

Soit $r = m - k$.

Posons :

$$\varepsilon : \prod_{1 \leq i \leq k} \mathbb{Z}/_{d_i\mathbb{Z}} \times \mathbb{Z}^r \longrightarrow \mathbb{Z}^m/_{\operatorname{Ker} f}$$

$$(\dot{t}_1, \dots, \dot{t}_k, t_{k+1}, \dots, t_m) \longmapsto \overline{\sum t_i e_i}$$

Vérifions que, si $\dot{t}_1 = \dot{t}'_1$ et ... $\dot{t}_k = \dot{t}'_k$, alors $\overline{\sum_1^k t_i e_i} = \overline{\sum_1^k t'_i e_i}$

$\dot{t}_i = \dot{t}'_i \Leftrightarrow d_i | t_i - t'_i \Leftrightarrow t'_i = t_i + d_i \lambda$

et $t'_i e_i = t_i e_i + \lambda \underbrace{d_i e_i}_{\in \operatorname{Ker} f} \Rightarrow \overline{t'_i e_i} = \overline{t_i e_i}$

$\varepsilon$ est un morphisme surjectif.
Est-il injectif ?

$$\overline{\sum t_i e_i} = \dot{0} \Leftrightarrow \exists \lambda_1, \dots, \lambda_k \in \mathbb{Z} \,/\, \sum_{i=1}^{m} t_i e_i = \sum_{j=1}^{k} \lambda_j d_j e_j$$

$$\Leftrightarrow \begin{cases} t_j = \lambda_j d_j \text{ si } j \leq k \Leftrightarrow \dot{t}_j = \dot{0} \\ t_j = 0 \quad \text{si } j > k \end{cases}$$

oui.

• unicité

Notons $\Gamma = \left(\prod_{1 \leq i \leq k} \mathbb{Z}/_{d_i \mathbb{Z}}\right) \times \mathbb{Z}^r \simeq G$

et $\Gamma' = \left(\prod_{1 \leq i \leq l} \mathbb{Z}/_{d'_i \mathbb{Z}}\right) \times \mathbb{Z}^s$

et supposons que $\Gamma' \xrightarrow{\sim} G$ avec $d'_i > 0$ $\quad d'_i \mid d'_{i+1}$

Alors montrons que $r = s$, $l = k$ et $d_i = d'_i$ $\quad \forall i \in [1, k]$

a) $r = s$

On a $\Gamma \simeq G \simeq \Gamma'$, et l'on sait que $\forall a \in \mathbb{Z}$ $\quad a\Gamma \simeq a\Gamma'$

Prenons $a = d_k \times d'_l$

$\forall i \quad d_i \mid d_k \Rightarrow d_i \mid d_k d'_l$ donc $a\Gamma \simeq a\mathbb{Z}^r \simeq \mathbb{Z}^r$

De même $a\Gamma' \simeq a\mathbb{Z}^s \simeq \mathbb{Z}^s$

et $a\Gamma \simeq a\Gamma' \Rightarrow \mathbb{Z}^r \simeq \mathbb{Z}^s \Rightarrow r = s$ (ce sont des ga ltf)

CQFD

b) **lemme** $a, d \in \mathbb{N} \setminus \{0\}$ alors $\#\left(a\, \mathbb{Z}/_{d\mathbb{Z}}\right) = \dfrac{d}{\Delta(a, d)}$

En effet $a\, \mathbb{Z}/_{d\mathbb{Z}}$ = le sous-groupe de $\mathbb{Z}/d\mathbb{Z}$ engendré par $\dot{a}$.

Et $\omega(\dot{a}) = \dfrac{d}{\Delta(a, d)}$ :

$r\dot{a} = \dot{0} \Leftrightarrow ra = \lambda d \Leftrightarrow ra' = \lambda d'$ où $\begin{cases} d = \Delta(a, d)\, d' \\ a = \Delta(a, d)\, a' \end{cases}$

$\Downarrow$

$d' \mid r$

Comme $d'\dot{a} = \dot{0}$, on en déduit $\omega(\dot{a}) = d'$.

c) Montrons que $\underbrace{\prod_{1\leq i\leq k} \mathbb{Z}/d_i\mathbb{Z}}_{T(\Gamma)} \simeq \underbrace{\prod_{1\leq i\leq l} \mathbb{Z}/d'_i\mathbb{Z}}_{T(\Gamma')}$ (groupes de torsion)

$T(\Gamma) = \{x\in\Gamma \,/\, \exists \lambda \neq 0,\ \lambda x = 0\}$ ? (1)

(ensemble des éléments d'ordre fini de $\Gamma$)

Si $x\in T(\Gamma)$, alors $d_k x = 0$

Si $x\in\Gamma \,/\, \lambda x = 0$ $(\lambda\neq 0)$

alors $\lambda x = (\lambda \dot{t}_1, \ldots, \lambda \dot{t}_k, \lambda t_{k+1}, \ldots, \lambda t_m) = (0, \ldots, 0)$

$$\Downarrow$$

$$t_{k+1} = \ldots = t_m = 0$$

donc $x\in T(\Gamma)$. (1) est montré.

Alors : $\Gamma\simeq\Gamma' \Rightarrow T(\Gamma)\simeq T(\Gamma')$ car un isomorphisme conserve les ordres des éléments (et, en particulier, la finitude de ces ordres).

d) $d_k = d'_l$

Compte tenu de c)

$$d_k T(\Gamma) = 0 \Rightarrow d_k T(\Gamma') = 0 \Rightarrow d'_1, \ldots, d'_l \mid d_k$$
$$\Rightarrow d'_l \mid d_k$$

Inversement, $d_k \mid d'_l$, donc $d_k = d'_l$

e) $d_i = d'_i$ par récurrence

$$\# \, d_{k-1} T(\Gamma) = \# \, d_{k-1} \mathbb{Z}/d_k\mathbb{Z} = \frac{d_k}{d_{k-1}}$$

$$\# \, d_{k-1} T(\Gamma') = \underbrace{\prod_{1\leq i\leq l-1} \frac{d'_i}{\Delta(d'_i, d_{k-1})}}_{\text{(cf lemme)}} \cdot \underbrace{\frac{d_k}{\Delta(d_{k-1}, d_k)}}_{=\frac{d_k}{d_{k-1}}}$$

ces cardinaux sont égaux car $T(\Gamma)\simeq T(\Gamma')$ (cf c))

Donc : $\forall i \in [1, \ell-1]$ $\quad d'_i = \delta(d'_i, d_{k-1})$

$$\Downarrow$$

$$d'_i \mid d_{k-1}$$

En particulier $d'_{\ell-1} \mid d_{k-1}$.

De m̂ $d_{k-1} \mid d'_{\ell-1} \Rightarrow d_{k-1} = d'_{\ell-1}$

(récurrence décroissante)

CQFD

# Décomposition d'un groupe en composantes p-primaires

## 1% Décomposition en composantes p-primaires.

**Def** | $G$ est appelé p-groupe ou "groupe p-primaire" si $\# G = p^n$ (où $p$ premier)

**Th** | Tout groupe abélien fini se décompose en produit de groupes p-primaires, et de manière unique.

$$\boxed{G = \bigoplus_j G(p_j)}$$

où $\# G(p_j) = p_j^{k_j}$, $n = p_1^{k_1} \cdots p_k^{k_k}$

Preuve :

$$G \simeq \prod_{1 \leq i \leq k} \mathbb{Z}/d_i\mathbb{Z} \quad \text{et} \quad d_i = \prod_{1 \leq j \leq k} p_j^{\alpha_{ij}}$$

Le théorème chinois donne :

$$\mathbb{Z}/d_i\mathbb{Z} \simeq \prod_{1 \leq j \leq k} \left( \mathbb{Z}/p_j^{\alpha_{ij}}\mathbb{Z} \right)$$

Donc

$$G \simeq \prod_{i,j} \mathbb{Z}/p_j^{\alpha_{ij}}\mathbb{Z} = \prod_j \Big( \underbrace{\prod_i \mathbb{Z}/p_j^{\alpha_{ij}}\mathbb{Z}}_{G(p_j)} \Big)$$

où $\# G(p_j) = p_j^{\sum_i \alpha_{ij}}$. Donc $G \simeq \prod_j G(p_j)$

$G(p_j)$ est un $p_j$-groupe

Remarque

$$G \simeq \prod_j G(p_j) \quad \text{où} \quad \# G(p_j) = p_j^{k_j} \quad \text{si} \quad n = \prod_j p_j^{k_j}$$

En effet : on a $G \simeq \prod_\ell \Big( \underbrace{\prod_i \mathbb{Z}/_{p_\ell^{\alpha_{i\ell}}\mathbb{Z}}}_{G(p_\ell)} \Big)$ et $\# G(p_\ell) = p_\ell^{\sum \alpha_{i\ell}}$

d'où $n = \# G = \prod_\ell p_\ell^{\sum_i \alpha_{i\ell}}$

La décomposition de $n$ en produit de facteurs premiers est unique, d'où $p_\ell = p_j$ et $\sum_i \alpha_{i\ell} = k_j$. (oui)

Exo : Montrer que, si $j \neq k$, $G(p_j) \cap G(p_k) = \{0\}$. En déduire que $G(p_j) + G(p_k) = G(p_j) \oplus G(p_k)$

Remarque : $G = \bigoplus_{j=1}^{k} G(p_j) = \bigoplus_{j=1}^{\ell} G(p'_j) \Rightarrow n = \prod_1^k p_j^{\alpha_j} = \prod_1^\ell p_j'^{\alpha'_j} \Rightarrow p_j = p'_j$ et $k = \ell$.

d'où l'unicité

2°/ Recherche du nombre de groupes abéliens finis à $n$ éléments

1) Si $n$ est premier, il n'y en a qu'un : $\mathbb{Z}/_{n}\mathbb{Z}$

2) Si $n = p^k$ où $p$ = nbre premier (c.à.d. si $G$ est un $p$-groupe)

D'après le th. fond. des gatf :

$$G \simeq \prod_i \mathbb{Z}/_{d_i\mathbb{Z}} \quad \text{où} \quad \prod d_i = p^k \Rightarrow \forall i \quad d_i = p^{\alpha_i}$$

$(\alpha_i \leq \alpha_{i+1})$

et $\sum \alpha_i = k$

On vérifie qu'il y a autant de groupes abéliens à $n$ éléments que de suites $(\alpha_i)$ croissantes, finies et dans $\mathbb{N}$ ; et vérifiant :

$\sum \alpha_i = k$

Notons $\rho(k) = \#\left\{ (\alpha_1, \dots, \alpha_{k'}) \ / \ \begin{matrix} \alpha_i \in \mathbb{N} \\ \alpha_i \leq \alpha_{i+1} \end{matrix} \text{ et } \sum_1^{k'} \alpha_i = k \right\}$

et notons $\alpha(p^k)$ le nombre de groupes abéliens finis à $p^k$ éléments.

Alors :

$$\boxed{\alpha(p^k) = \rho(k)}$$

3) Si n quelconque

Alors

$$G \simeq \prod_j G(p_j) \quad \text{où} \quad \# G(p_j) = p_j^{k_j}$$

Il y a $\rho(k_j)$ possibilités pour $G(p_j)$, d'où $\alpha(n) = \prod_j \rho(k_j)$

$$\boxed{\alpha(n) = \prod_j \rho(k_j) \ , \text{si } n = \prod_j p_j^{k_j}}$$

que l'on peut aussi écrire : $\alpha(n) = \prod_j \alpha\left( p_j^{\nu_{p_j}(n)} \right)$

3°/ Etude de $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$

$$\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) = \{ x \in \mathbb{Z}/n\mathbb{Z} \ / \ \exists y \in \mathbb{Z}/n\mathbb{Z} \quad xy = 1 \}$$

* Si n est premier, on sait que $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ est cyclique à $n-1$ éléments.

* Si $n = p^k$

Alors $\# \mathcal{U}(\mathbb{Z}/n\mathbb{Z}) = \varphi(n) = \varphi(p^k) = p^{k-1}(p-1)$

$\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ est un groupe abélien à $p^{k-1}(p-1)$ éléments.

**Lemme** Pour $n = p^k$, il existe dans $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ un élément d'ordre $(p-1)$ et un élément d'ordre $p^{k-1}$, si $p \neq 2$

Preuve :

* Soit le morphisme $\mathbb{Z}/p^k\mathbb{Z} \xrightarrow{f} \mathbb{Z}/p\mathbb{Z}$, $\dot{x} \longmapsto \ddot{x}$

$f$ est surjective,

Donc $\tilde{f} : \mathcal{U}(\mathbb{Z}/p^k\mathbb{Z}) \to \mathcal{U}(\mathbb{Z}/p\mathbb{Z})$ est un morphisme surjectif

$\exists y \in \mathcal{U}(\mathbb{Z}/p\mathbb{Z}) \ / \ \omega(y) = p-1$

Et donc, si $x \in \mathcal{U}(\mathbb{Z}/p^k\mathbb{Z})$ tel que $f(x) = y$

$$\omega(y) \mid \omega(x) \Rightarrow (p-1) \mid \omega(x) \Rightarrow \omega(x) = \lambda(p-1)$$

d'où $\omega(x^\lambda) = p-1$

* Montrons que :

$$\forall p > 2 \quad (1+p)^{p^k} \equiv 1 + p^{k+1} \ [p^{k+2}]$$

Vrai pour $k=0$.

Vrai au rang $k$, alors :

$$\begin{aligned}(1+p)^{p^{k+1}} &= \left[(1+p)^{p^k}\right]^p \\ &= \left[1 + p^{k+1} + \lambda p^{k+2}\right]^p \qquad (\lambda \in \mathbb{Z}) \\ &= (1+p^{k+1})^p + \underbrace{p(1+p^{k+1})^{p-1}\lambda p^{k+2} + \ldots}_{\equiv 0 \ [p^{k+3}]}\end{aligned}$$

d'où :

$$\begin{aligned}(1+p)^{p^{k+1}} &\equiv (1+p^{k+1})^p \quad [p^{k+3}] \\ &\equiv 1 + p^{k+2} + \underbrace{C_p^2 \, p^{2(k+1)}}_{\equiv 0} + \underbrace{\ldots}_{\equiv 0} \quad [p^{k+3}]\end{aligned}$$

d'où $(1+p)^{p^{k+1}} \equiv 1 + p^{k+2} \ [p^{k+3}]$ oui.

Alors : $\begin{cases} (1+p)^{p^{k-2}} \equiv 1 + p^{k-1} & [p^k] \\ (1+p)^{p^{k-1}} \equiv 1 + p^k & [p^{k+1}] \end{cases}$

d'où $\begin{cases} (\dot{\overline{1+p}})^{p^{k-2}} = \dot{1} + \dot{p}^{k-1} \neq \dot{1} & \text{dans } \mathbb{Z}/_{p^k}\mathbb{Z} \\ (\dot{\overline{1+p}})^{p^{k-1}} = \dot{1} \end{cases}$

$$\Downarrow$$

$(\dot{\overline{1+p}})$ est d'ordre $p^{k-1}$ dans $\mathbb{Z}/_{p^k}\mathbb{Z}$

CQFD

**Th** | Soit $p \neq 2$ un nombre premier.
$\mathcal{U}(\mathbb{Z}/_{p^k}\mathbb{Z})$ est cyclique de cardinal $\varphi(p^k) = (p-1)\,p^{k-1}$

Preuve : D'après le lemme :

$\exists x \in \mathbb{Z}/_{p^k}\mathbb{Z} \ / \ \omega(x) = p-1$

$\exists y \in \mathbb{Z}/_{p^k}\mathbb{Z} \ / \ \omega(y) = p^{k-1}$

Donc $\omega(xy) = p^{k-1}(p-1) = \# \mathcal{U}(\mathbb{Z}/_{p^k}\mathbb{Z})$

↑ parceque $\Delta(\omega(x), \omega(y)) = 1$ (voir NB)

<u>NB</u> : Soit $G$ un groupe abélien.

Soient $x, y \in G \ / \ \Delta(\omega(x), \omega(y)) = 1$. Alors $\omega(xy) = \omega(x)\,\omega(y)$

En effet :

Soient $G_x$ et $G_y$ les sous-groupes engendrés respectivement par $x$ et par $y$. Alors $G_x \cap G_y = \{0\}$ car $z \in G_x \cap G_y \Rightarrow \omega(z) \mid \omega(x)$ et $\omega(z) \mid \omega(y) \Rightarrow \omega(z) = 1 \Rightarrow z = 0$. Donc $G_x + G_y = G_x \oplus G_y$ et $G_x \oplus G_y \simeq G_x \times G_y$

$$\Downarrow$$

$$\omega(x+y) = \underbrace{\omega(x,y)} = \text{ppcm}(\omega(x), \omega(y)) = \omega(x)\,\omega(y)$$

d'où $\omega(x+y) = \omega(x)\,\omega(y)$

CQFD

Dans le cas où $p=2$, on a le théorème :

Th | $\mathcal{U}(\mathbb{Z}/4\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$
Mais :
$\forall k \geq 3 \quad \mathcal{U}(\mathbb{Z}/2^k\mathbb{Z}) \simeq \mathbb{Z}/2^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Preuve :

On a $\mathcal{U}(\mathbb{Z}/4\mathbb{Z}) = \{1, 3\}$ et $3^2 = 1$, d'où $\mathcal{U}(\mathbb{Z}/4\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$

Mais $\mathcal{U}(\mathbb{Z}/8\mathbb{Z}) = \{1, 3, 5, 7\}$ et $3^2 = 1$ ; $5^2 = 7^2 = 1$.

Donc :

$$\mathcal{U}(\mathbb{Z}/8\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{(groupe de Klein)}$$

On est amenés à montrer que

$$\forall k \geq 3 \quad \mathcal{U}(\mathbb{Z}/2^k\mathbb{Z}) \simeq \mathbb{Z}/2^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

1) $\mathcal{U}(\mathbb{Z}/2^k\mathbb{Z})$ est un galtf de cardinal $\varphi(2^k) = 2^{k-1}$. Donc tous ses éléments sont d'ordre $2^\alpha$ où $0 \leq \alpha \leq k-1$. En fait, il n'y a pas d'éléments d'ordre $2^{k-1}$ : Montrons que $x^{2^{k-2}} = \dot{1} \quad \forall k \geq 3$.
Récurrence sur $k \geq 3$. Pour $k = 3$, on a $x^2 = 1 \quad \forall x \in (\mathbb{Z}/8\mathbb{Z})^*$
Supposons que l'on ait $x^{2^{k-2}} = \dot{1} \quad [2^k]$.
Alors $x^{2^{k-1}} = (x^{2^{k-2}})^2 = (1 + 2^k q)^2 = 1 \quad [2^{k+1}]$
En conclusion, tous les éléments de $\mathcal{U}(\mathbb{Z}/2^k\mathbb{Z})$ sont d'ordre $2^\alpha$ où $0 \leq \alpha \leq k-2$.

2) Il existe un élément d'ordre $2^{k-2}$

- Pour $\mathbb{Z}/8\mathbb{Z} \quad \omega(\dot{5}) = 2$ car $\dot{5}^2 = \dot{1} \quad [8]$ ça marche.
- Montrons que $\omega(\dot{5}) = 2^{k-2} \quad \forall k \geq 3$.
  - C'est vrai pour $k = 3$.
  - Supposons que $\omega(\dot{5}) = 2^{k-2} \quad [2^k]$

$$\Updownarrow$$

$$\begin{cases} \dot{5}^{2^{k-2}} = \dot{1} & [2^k] \\ \dot{5}^{2^{k-3}} \neq \dot{1} & [2^k] \end{cases} \quad \text{(cf 1))}$$

Montrons alors que $\omega(\dot{5}) = 2^{k-1}$ dans $\mathcal{U}(\mathbb{Z}/_{2^{k+1}\mathbb{Z}})$

c.à.d que : $\begin{cases} \dot{5}^{2^{k-1}} = \dot{1} \quad [2^{k+1}] \\ \text{et} \\ \dot{5}^{2^{k-2}} \neq \dot{1} \quad [2^{k+1}] \end{cases}$

On a :

$$5^{2^{k-2}} = 1 + 2^{k} q \Rightarrow 5^{2^{k-1}} = (1+2^k q)^2 \equiv 1 \quad [2^{k+1}]$$

et

$$5^{2^{k-3}} \neq 1 \quad [2^k] \Leftrightarrow \forall q \in \mathbb{Z} \quad 5^{2^{k-3}} \neq 1 + 2^k q$$

$$\Downarrow$$

$$\forall q \quad 5^{2^{k-2}} \neq (1+2^k q)^2$$

$$\Downarrow$$

$$5^{2^{k-2}} \neq 1 \quad [2^{k+1}]$$

3) Comme $\mathcal{U}(\mathbb{Z}/_{2^k\mathbb{Z}})$ est un gaAF qui possède un élément d'ordre $2^{k-2}$ et comme $\mathcal{U}(\mathbb{Z}/_{2^k\mathbb{Z}}) \not\simeq \mathbb{Z}/_{2^{k-1}\mathbb{Z}}$, on a :

$$\mathcal{U}(\mathbb{Z}/_{2^k\mathbb{Z}}) \simeq \prod_{i=1}^{\ell} \mathbb{Z}/_{2^{\alpha_i}\mathbb{Z}}$$

$$\simeq \underbrace{\mathbb{Z}/_{2^{k-2}\mathbb{Z}}}_{\text{car } \exists \text{ élément d'ordre } 2^{k-2}} \times \mathbb{Z}/_{2^\alpha\mathbb{Z}} \qquad \text{où } 2^\alpha \mid 2^{k-1}$$

$$\Downarrow$$

$$\alpha \leq k-1$$

Or, en passant aux cardinaux : $2^{k-1} = 2^{k-2} \cdot 2^\alpha \Rightarrow \alpha = 1$.

D'où :

$$\boxed{\mathcal{U}(\mathbb{Z}/_{2^k\mathbb{Z}}) \simeq \mathbb{Z}/_{2^{k-2}\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}} \qquad \underline{k \geq 3}$$

# 3 Polynômes à 1 ou 2 variables.

$K[X]$ et $\mathbb{Z}$ se ressemblent beaucoup : ce sont tous les deux des "anneaux euclidiens" (c.à.d des anneaux principaux et admettant une division euclidienne)

## Anneau des polynômes $K[X]$

$K$ = anneau commutatif unitaire.

Def : On appelle polynôme à 1 variable, à coefficients dans $K$, une suite $(a_0, a_1, \ldots, a_i, \ldots) \in K^{\mathbb{N}}$ telle que
$$\exists n \in \mathbb{N} \ / \ i > n \Rightarrow a_i = 0$$

Rappelons que :

$(K[X], +, .)$ = espace vectoriel sur $K$ (si $K$ = corps)

$(K[X], +, \times)$ = anneau commutatif unitaire

Rappels : 1) $\deg(P+Q) \leq \text{Sup}(\deg P, \deg Q)$

2) $\deg(PQ) \leq \deg P + \deg Q$ ($K$ anneau)

3) Si $K$ est intègre, alors $\deg PQ = \deg P + \deg Q$

4) Si $K$ est intègre, alors $P$ inversible $\Rightarrow P$ = constante.

(Sol : $P$ inv. $\Rightarrow \exists Q \ / \ PQ = 1 \Rightarrow \deg P + \deg Q = 0 \Rightarrow \deg P = \deg Q = 0$

5) Si $K$ est intègre, alors $K[X]$ est intègre.

Comme nous avions fait dans $\mathbb{Z}$, on peut parler d'idéaux dans $K[X]$
Rappelons la définition d'un idéal $I$ d'un anneau commutatif $A$ :

• $(I,+)$ = sous-groupe de $A$.
• $\forall x \in A \quad \forall i \in I \quad xi \in I$ } $\Leftrightarrow$ $I$ idéal de $A$.

On sait que l'idéal engendré par un élément $x$ d'un anneau $A$ commutatif et unitaire nous est donné par :

$$(x) = xA = \{ z \in A \,/\, \exists y \in A \quad z = xy \}$$

(voir Lueysanne)

Def : $A, B \in K[X] \qquad A \mid B \Leftrightarrow (B) \subset (A)$

En d'autre termes, $A$ divise $B$ ssi $\exists Q \in K[X]$ tel que $B = AQ$

Exo : $K$ = anneau. Soit $I \subset K$. Alors $I$ idéal $\Leftrightarrow$ $I$ = sous-module de $K$

## K intègre : division euclidienne dans $K[X]$

($K$ = anneau commutatif intègre)

Th | $A, B \in K[X]$ et $B \neq 0$ tel que $b_q$ inversible dans $K$ ($\deg B = q$)
$\exists!\ (Q, R) \in (K[X])^2$ tels que
$$A = BQ + R \quad \text{où} \quad R = 0 \text{ ou } \deg R < \deg B$$

Preuve :

• Unicité : $\begin{cases} A = BQ + R \\ A = BQ' + R' \end{cases}$

$$B(Q - Q') = R' - R$$

et $\begin{cases} \deg(R' - R) \leqslant \operatorname{Sup}(\deg R, \deg R') < \deg B & \text{si } R \neq R' \\ \deg B(Q - Q') \geqslant \deg B & \text{si } Q \neq Q' \end{cases}$

absurde. Donc $Q = Q'$ et $R = R'$

• Existence :

Posons $\deg A = p$ et $\deg B = q$

* Si $p<q$, je prends $Q=0$ et $R=A$
* Si $p \geq q$, et si $Q$ existe, alors $\deg Q = p-q = n$

$$\begin{cases} Q = c_0 + c_1 X + \dots + c_n X^n \\ A = a_0 + \dots + a_p X^p \\ B = b_0 + \dots + b_q X^q \end{cases}$$

$$A = BQ + R \Rightarrow \begin{cases} a_p = b_q c_n \\ \text{------} \\ a_q = b_q c_0 + b_{q-1} c_1 + \dots + b_0 c_q \end{cases}$$

C'est un système diagonal qui se résoud de proche en proche car $b_q \in K^*$. On trouve ainsi $Q$, et $R = A - BQ$ qui sera bien tel que $\deg R < q$

$K$ = corps ssi $K[X]$ principal

Th | $K$ est un corps $\Leftrightarrow$ $K[X]$ principal

(Rappel : $A$ anneau principal ssi tout idéal y est principal, c.à.d $\forall I$ idéal de $A$ $\exists a \in A$ / $(a) = I$ )

Preuve :

($\Rightarrow$) Soit $A \in I \subset K[X]$ de degré minimum. $\forall B \in I$ :
$B = AQ + R$ où $R = 0$ ou $\deg R < \deg A$.
Si $R \neq 0$, $R = B - AQ \in I$ et de degré inférieur à celui de $A$. C'est absurde.
Donc $R = 0 \Rightarrow B = AQ \Rightarrow I = (A)$

($\Leftarrow$) Si $K \neq$ corps, alors il existe un idéal $I$ non trivial (c.à.d tel que $I \neq 0$ et $K$)
En effet, sinon, pour $x \in K^*$ $(x) \neq (0) \Rightarrow (x) = (1)$

d'où $\exists y \,/\, xy = 1 \Rightarrow x$ inversible, et ceci $\forall x$. Absurde.

Montrons alors que $K \neq$ corps $\Rightarrow K[X] \neq$ anneau principal.

Considérons, pour cela $J = \{P \in K[X] \,/\, P(0) \in I\}$ où $I$ est un ideal non trivial de $K$. Alors $J = (X) + (\text{cte de } I)$

CQFD

Exo : Montrer que $\mathbb{Z}[X]$ n'est pas principal.

(Sol : $I = \{P \,/\, P(0) \equiv 0 \; [3]\}$. Alors $3 \in I$ et $X \in I$ et de plus $I = (X) + (3)$. En effet $I \subseteq (X) + (3)$. et $(X) + (3) \neq (\text{Cte})$

$\forall P \in I \qquad P = 3a_n X^n + \dots + a_1 X + 3a_0$

$P = (a_n X^{n-1} + \dots + a_1) X + 3a_0 \Rightarrow I \subset (X) + (3)$

Exo : $K[X][Y] \doteq K[X,Y]$ n'est pas un anneau principal, et cela $\forall K$ corps ou anneau !

(Sol : * utiliser le théorème précédent

* Considérer $\mathcal{M} = \{P \in K[X,Y] \,/\, P(0,0) = 0\}$ non principal car $\mathcal{M} = (X) + (Y)$ )

## Fonction polynôme

$K$ = anneau

$$K \longrightarrow K$$
$$x \longmapsto P(x) = \sum_{i=0}^{n} a_i x^i$$

$$\text{où } P(X) = \sum_{i=0}^{n} a_i X^i.$$

On note $\varphi : K[X] \longrightarrow K^K$

$P \longmapsto \varphi(P)$ défini ci-dessus.

ainsi : $\varphi(P)(x) = P(x)$

Problème : Quand est-ce que $\varphi$ est injective ?

* Contre-exemple 1 : Si $K$ est un corps fini, $\varphi$ n'est pas injective.
Prenons $K = \mathbb{Z}/7\mathbb{Z}$
Alors $X^7 - X \neq 0$ et pourtant $\forall x \in \mathbb{Z}/7\mathbb{Z} \quad x^7 - x = 0$
(cf. Th. de Fermat)

* Contre-exemple 2 : Si $K$ est un anneau infini, mais non intègre, $\varphi$ n'est pas injective.
En effet, dans l'anneau de Boole $(\mathcal{P}(E), \Delta, \cap) = A$ où $E$ est un ensemble infini, on a :

$$\forall X \in A \qquad X^2 = X$$

Le polynôme $X^2 - X$ définit la fonction nulle

Avant de donner une condition nécessaire pour que $\varphi$ soit injective, démontrons les 2 lemmes suivants :

Lemme 1 : Soit $K$ un anneau commutatif.
Alors $a \in K$ est racine de $P \Leftrightarrow P(X) \in (X-a) \subset K[X]$

Lemme 2 : Si $K$ est un anneau intègre(*), et si $P \in K[X]$ est de degré $n$ ($P \neq 0$), alors $P$ possède au plus $n$ racines dans $K$.

Preuves :
- lemme 1 :

$$(\Rightarrow) \begin{cases} P(X) = \sum_{i=0}^{n} a_i X^i \\ P(a) = 0 \end{cases} \qquad \text{d'où :}$$

(*) : on dit qu'un anneau $A$ est intègre si :
1) il est commutatif
2) et $ab = 0 \Rightarrow a = 0$ ou $b = 0$.

$$P(X) - P(a) = \sum_{i=0}^{n} a_i (X^i - a^i) = (X-a) \sum_{i=0}^{n} a_i \Big( \sum_{j=0}^{i-1} a^{i-1-j} X^j \Big)$$

donc $\quad P(X) = (X-a)\, Q(X) \Rightarrow P(X) \in (X-a)$

($\Leftarrow$) Inversement, si $P(X) = (X-a)\,Q(X)$ alors $P(a) = 0$.

oui.

△ lemme 2 :

- $n = 0$ pas de racines
- $n = 1 \quad P(X) = aX + b \quad (a \neq 0)$

Alors $\quad a(x - x') = 0 \Rightarrow x = x'$ car $K$ intègre. ce qui montre que $P(X)$ a au plus une racine.

Remarquons que $P(X) = aX + b$ n'a pas de racine si $X$, et possède une racine unique si $1$.

- Vrai pour $n \Rightarrow$ vrai pour $n+1$ ?

Soit $P$ / $\deg P = n+1$.

Si $P$ n'a pas de racines, c'est fini.

Sinon, soit $a$ l'une de ses racines. Alors $P(X) \in (X-a)$ (cf. lemme 1) donc $\exists Q \in K[X]$ / $P(X) = (X-a)\,Q(X)$ et $\deg Q = n$, donc $Q$ possède au plus $n$ racines.

CQFD

**Th** | Soit $\varphi : K[X] \longrightarrow K^K$
Si $K$ intègre infini, alors $\varphi$ est injective.

Preuve :

$$\varphi(P) = \varphi(P') \Leftrightarrow \forall x \in K \quad P(x) = P'(x)$$
$$\Leftrightarrow \forall x \in K \quad (P - P')(x) = 0$$

Si $P - P' \neq 0$, alors $P - P'$ possède une infinité de racines et pourtant (car $K$ intègre) il doit posséder au plus $n$ racines ! Absurde. Donc $P - P' = 0$. CQFD

$aX^2+bX+c$

2) Sur $\mathbb{Q}$ $\quad r \in (\mathbb{Q}^*)^2 \Leftrightarrow \forall p \in \mathcal{P} \quad v_p(r) \equiv 0\ [2]$

3) Sur $\mathbb{R}$ $\quad (\mathbb{R}^*)^2 \simeq \mathbb{R}_+^*$ $\qquad$ (lire $(\mathbb{R}^*)^2$ = quarrés d'él. de $\mathbb{R}^*$)

4) Sur $\mathbb{C}$ $\quad (\mathbb{C}^*)^2 \simeq \mathbb{C}^*$ ①

Th ③ | Soit $P \in \mathbb{R}[X]$
deg $P$ impair $\Rightarrow$ $P$ a une racine dans $\mathbb{R}$

Considérer $x \mapsto P(x) = a_{2n+1} x^{2n+1} + \dots$

Si $a_{2n+1} > 0$ $\begin{cases} \lim_{+\infty} P(x) = +\infty \\ \lim_{-\infty} P(x) = -\infty \end{cases}$

$P(x)$ est continue

Le th. de la valeur intermédiaire

montre que $\exists c \in \mathbb{R} \,/\, P(c) = 0$.

Théorème de D'Alembert-Gauss.

Th | $\sim$
a) Tout polynôme de $\mathbb{C}[X]$ (de degré $\geq 1$) admet une racine dans $\mathbb{C}$
b) Les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes du 1-degré.
c) Tout polynôme de $\mathbb{R}[X]$ a une racine dans $\mathbb{C}$

$*$ $\sim$ ?

a $\Rightarrow$ c) évident

a $\Rightarrow$ b) utiliser le lemme 1

b $\Rightarrow$ a) récurrence sur le degré

c $\Rightarrow$ a) $\quad P \in \mathbb{C}[X] \qquad Q = P\bar{P} \in \mathbb{R}[X]$

(En effet, $R \in \mathbb{C}[X]$ $\quad R \in \mathbb{R}[X] \Leftrightarrow \bar{R} = R$ )

D'après le c) $\exists \alpha \in \mathbb{C} \,/\quad P(\alpha)\,\bar{P}(\alpha) = 0$

Si $P(\alpha) = 0$, c'est fini.

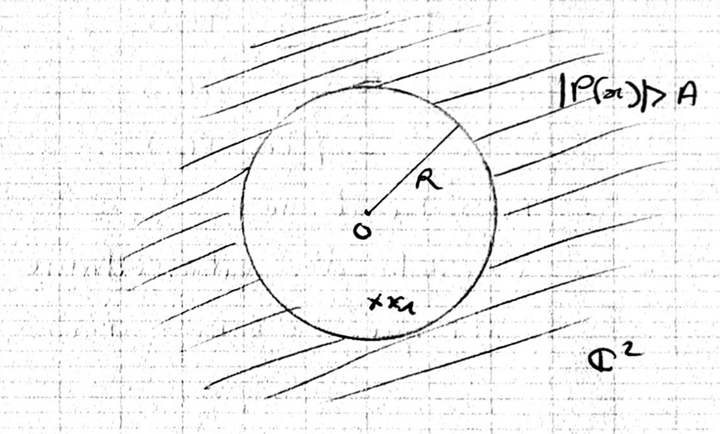
Sinon $\bar{P}(\alpha) = 0 \Rightarrow \overline{\bar{P}(\alpha)} = 0 = P(\bar{\alpha})$ donc $\bar{\alpha}$ est racine.

* Preuve de $\alpha)$

Soit $P \in \mathbb{R}[X]$ $\qquad P(x) = a_n x^n + \dots + a_0$

$$x \longmapsto P(x)$$
$$\mathbb{C} \longrightarrow \mathbb{C}$$

Si $P$ n'a pas de racine, $\forall x \in \mathbb{C} \quad |P(x)| > 0$




$\exists x_1 \,/\quad |P(x_1)| = \inf\limits_{x \in \mathbb{C}} |P(x)|$

On peut se ramener au cas où $x_1 = 0$ et où $|P(x_1)| = 1$

(Poser $Q = P(x + x_1)$ et diviser correctement)

Donc :

$$Q(x) = 1 + a_n x^n + x^{n+1} R(x)$$
$$(\text{où } a_n \neq 0)$$

On va montrer que c'est impossible :

$$Q(x) = 1 + a_r x^r + x^{r+1} R(x)$$

Si nous montrions que :

$\exists x \quad |1 + a_r x^r| < 1 - 2\varepsilon$ et $|x R(x)| < \varepsilon$ où $\varepsilon > 0$.

on aura :

$$|Q(x)| < |1 + a_r x^r| + |x R(x)|$$
$$< 1 - 2\varepsilon + \varepsilon < 1 - \varepsilon$$ , d'où l'absurdité puisque $1 = \inf_{x \in \mathbb{C}} |P(x)|$.

On a :

$$a_r x^r \in \mathbb{R}_- \Leftrightarrow \operatorname{Arg}(a_r x^r) \equiv \pi \quad [2\pi]$$
$$\Leftrightarrow \operatorname{Arg} a_r + r \operatorname{Arg} x \equiv \pi \quad [2\pi]$$
$$\Leftrightarrow \theta = \operatorname{Arg} x \equiv \frac{1}{r}(\pi - \operatorname{Arg} a_r) \quad \left[\frac{2\pi}{r}\right]$$

On choisit ce $\theta$. Alors $a_r x^r \in \mathbb{R}_-$. On choisit enfin le module de $x$ de façon à ce que $x^{r+1} R(x)$ ne compense pas ce $a_r x^r$, c.à.d. tel que

$$2|x^{r+1} R(x)| < |a_r x^r| \Leftrightarrow |a_r| > 2|x||R(x)|$$
$$\Leftarrow |x| < \frac{1}{2}\frac{|a_r|}{M}$$

$\begin{cases} \text{où } |R(x)| < M \\ x \in V_0 \text{ voisinage de } 0 \end{cases}$

Alors $a_r x^r \in \mathbb{R}^-$, c.à.d $a_r x^r = -2\varepsilon$ où $\varepsilon \in \mathbb{R}_+^*$

et $2|x^{r+1} R(x)| < 2\varepsilon \Rightarrow |x^{r+1} R(x)| < \varepsilon$

CQFD

Modules sur $K[X]$

$E$ est un $A$-module, où $A$ est un anneau commutatif unitaire, si $E$ est un groupe abélien et si $A \times E \to E$
$(a, e) \mapsto ae$
possède les 4 propriétés habituelles des e.v.

Prenons $A = K[X]$. Soit $E$ un $K$-module.
$a_i e$ est bien défini ($a_i \in K$).
Comment définir $Xe$ ? On veut que $\begin{cases} X(e'+e'') = Xe' + Xe'' \\ X(ae) = a(Xe) \end{cases}$
donc $e \mapsto Xe$ est un endomorphisme de $K$-modules.

→

| |
|---|
| En fait<br>$K[X]$-module sur $E$ $\Longleftrightarrow$ $\begin{cases} K\text{-module sur } E \\ \text{et} \\ \exists \text{ endomorphisme } K\text{-linéaire de } E \end{cases}$ |

~~Graphique ⇒~~. Montrons $\Leftarrow$. (⇒ évident)

$\begin{cases} E = K\text{-module} \\ u \in \mathrm{End}_K(E) \end{cases}$

$(\sum a_i X^i)e \doteq \sum a_i u^i(e)$ où $u^i = \underbrace{u \circ u \circ \dots \circ u}_{i \text{ fois}}$
qui définit bien une loi externe dans $E$, pour $K[X]$.

**Th** | $K$ corps. Soit $E$ un ev sur $K$, et $u \in \mathcal{L}(E,E)$
Alors
$(E, u)$ a une structure de $K[X]$ module sur $E$
grâce à $(\sum_i a_i X^i)e = \sum_i a_i u^i(e) \in E$
c.à.d $P.e \doteq P(u)e$

(Ainsi, si $E$ = ev sur $K$
$E = K[X]$-module $\Leftrightarrow$ $(E, u)$ où $u \in \mathcal{L}(E)$ )

Soit E un K-e.v. et $u \in \mathcal{L}(E)$. $(E,u)$ est un $K[X]$-module grâce au produit $P.x = P(u)x$ $\forall x \in E$

**Sous-$K[X]$-modules de E**

Si $F \subset E$ est un sev invariant par u, alors :

$$\forall x \in F \quad u(x) \in F$$

Et donc $\forall x \in F$ $\forall P \in K[X]$ $P(u)x = P.x \in F$

En d'autres termes, F est un sous-$K[X]$-module de $(E,u)$

**Automorphisme de $K[X]$-module**

$(E,u) \simeq (E,v) \iff \exists \varphi : E \to E$ qui soit $K[X]$-linéaire bij.

c.à.d : $\begin{cases} \forall e, e' \in E \quad \varphi(e+e') = \varphi(e) + \varphi(e') \\ \forall P \in K[X] \quad \forall e \in E \quad \varphi(Pe) = P\varphi(e) \end{cases}$

$$\Updownarrow$$

$\begin{cases} \varphi(e+e') = \varphi(e) + \varphi(e') \text{ et } \varphi(ae) = a\varphi(e) \\ \varphi(Xe) = X\varphi(e) \iff \varphi \circ u = v \circ \varphi \end{cases}$

$$\Updownarrow$$

$\begin{cases} \varphi \text{ est } K\text{-linéaire bijective,} \\ \varphi \circ u = v \circ \varphi \text{ , c.à.d } u \text{ et } v \text{ sont semblables.} \end{cases}$

**Isomorphismes de $K[X]$-module**

Si $(E,u) \xrightarrow[\sim]{f} (E',u')$ est un isomorphisme de $K[X]$-modules, nous avons :

$$f \circ u = u' \circ f \quad \text{et } f \in \mathcal{L}(E,E') \text{ bijective}$$

$$\Updownarrow$$

$$u' = f \circ u \circ f^{-1}$$

(pas de dénomination).

Exo : Soit E un K-e.v. de dimension n, et $u \in End(E)$. Montrer qu'une base $(e_1, \dots, e_n)$ de E est un système générateur

de $E = K[X]$-module.

Sol : $\forall x \in E \quad \exists a_i \in K \ / \quad x = \sum_1^n a_i e_i$

$a_i \in K \hookrightarrow K[X]$, donc $(e_1, \dots, e_n)$ engendrent $E = K[X]$-module.

<u>Exemple</u> :

Prenons $E = K^2$ où $K$ = corps.

Considérons $u = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \qquad e_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad e_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

On a $\begin{cases} u(e_1) = e_2 \\ u(e_2) = e_1 + e_2 \end{cases}$

donc $(e_1, e_2)$ = ~~be~~ système générateur de $E = K[X]$-module.

On a $1.e_1 = e_1$

$X e_1 \doteq u(e_1) = e_2$

$\forall v \in E = K^2 \qquad v = a e_1 + b e_2 = \underbrace{(a + bX)}_{\in K[X]} e_1$

$(e_1)$ engendre $E$ où $E = K[X]$-module

Considérons $\varphi : K[X] \longrightarrow (E, u) \qquad E = K^2$

$$P \longmapsto P e_1$$

$$a + bX \longmapsto v = (a + bX) e_1$$

$\varphi$ est un morphisme surjectif de $K[X]$-modules et son noyau est $\operatorname{Ker} \varphi = \{ P \in K[X] / \ P e_1 = 0 \}$. Il n'est pas réduit à $0$ car :

$u^2(e_1) = e_1 + u(e_1) \Rightarrow u^2(e_1) - u(e_1) - e_1 = 0$

$\Rightarrow X^2 e_1 - X e_1 - e_1 = 0 \Rightarrow (X^2 - X - 1) \subset N$

Cherchons $N = \text{Ker}\,\varphi$. C'est un idéal de $K[X]$, et comme $K$ est un corps, $K[X]$ est principal, donc $\text{Ker}\,\varphi = (g)$. On va montrer que $N = (X^2 - X - 1)$

On a le diagramme :

$$N \hookrightarrow K[X] \overset{\varphi}{\twoheadrightarrow} (E, u)$$
$$P \longmapsto Pe_1$$

où $\varphi$ est un homomorphisme surjectif d'anneaux.

$\varphi$ "passe au quotient" car $(X^2 - X - 1) \subset N$ :

$$K[X]/(X^2-X-1) \overset{\bar{\varphi}}{\twoheadrightarrow} E \simeq K^2$$

$K[X]/(X^2-X-1)$ a une base $(\dot{1}, \dot{X})$. Ainsi $\bar{\varphi}$ est un hom. surjectif d'un ~~anneau~~ espace vectoriel $K[X]/(X^2-X-1)$ de ~~rang~~ dim 2 vers $E$ de ~~rang~~ dim 2. C'est un isomorphisme d'~~anneaux~~ espaces-vectoriels.

$$K[X]/(X^2-X-1) \simeq E$$

Donc $(X^2 - X - 1) = N$. En effet, nous avons, avec d'autres notations

$$A \overset{\varphi}{\twoheadrightarrow} A'$$

(diagramme : $A \to A/N \overset{\bar{\varphi}}{\to} A'$ ; $A \to A/\text{Ker}\,\varphi \overset{\tilde{\varphi}}{\to} A'$)

$N \subset \text{Ker}\,\varphi$ $\quad$ $\varphi$ hom. surj. d'anneaux.

Si $\bar{\varphi}$ est un isomorphisme d'anneaux alors $N = \text{Ker}\,\varphi$, puisque

$$\psi : A/\text{Ker}\,\varphi \overset{\sim}{\longrightarrow} A/N$$
$$\dot{x} \longmapsto \dot{x}_N$$

et : $\forall x \in \text{Ker}\,\varphi \Leftrightarrow \dot{x} = \dot{0} \Leftrightarrow \psi(\dot{x}) = \dot{x}_N = \dot{0} \Leftrightarrow x \in N$.

oui.

<u>$K[X]$-modules cycliques</u>

Un polynôme $P \in K[X]$ est dit "monique" s'il s'écrit :

$$P = X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0$$

Considérons $E = K[X]/_{(P)}$ .

Pro | $E = K[X]/_{(P)}$ est un $K$-espace vectoriel de dimension $n$, dont une base est $(\dot{1}, \dot{X}, \dots, \dot{X}^{n-1})$

$*$ $(K[X], +, .)$ = e.v. sur $K$, donc $(E, +, .)$ aussi (puisque $(P)$ est un idéal dans $K[X]$ : $\forall x \in (P)\ \forall \lambda \in K \quad \lambda x \in (P)$ )

$*$ $\lambda_i \in K \qquad \lambda_1 \dot{1} + \dots + \lambda_{n-1} \dot{X}^{n-1} = \dot{0}$

$$\Updownarrow$$

$$P \mid (\lambda_1 + \dots + \lambda_{n-1} X^{n-1})$$

Or $\deg P = n > n-1$, donc $\lambda_1 + \dots + \lambda_{n-1} X^{n-1} = 0 \Leftrightarrow \lambda_i = 0\ \forall i$

Le système $(\dot{1}, \dots, \dot{X}^{n-1})$ est donc libre. Montrons qu'il engendre $E$ ;

$\forall Q \in E \quad \deg Q = 0 \Rightarrow Q = Cte \Rightarrow \dot{Q} = cte$ s'exprime bien en fonction de $(\dot{1}, \dots, \dot{X}^{n-1})$.

Récurrence sur $\deg Q$ : Supposons que, $\forall Q \in E\ \deg Q = k$

$\Rightarrow \dot{Q} = \sum_{i=0}^{n-1} \lambda_i \dot{X}^i$

Soit $Q \,/\, \deg Q = k+1$

$$Q = \sum_{i=0}^{k+1} a_i X^i = \underbrace{\sum_0^k a_i X^i}_{\deg k} + X(\underbrace{a_{k+1} X^k}_{\deg k})$$

d'où

$$\dot{Q} = \sum_{i=0}^{n-1} \lambda_i \dot{X}^i + \dot{X}\left(\sum_{i=0}^{n-1} \mu_i \dot{X}^i\right)$$

$$\dot{Q} = \sum_{i=0}^{n-1} \lambda_i \dot{X}^i + \sum_{i=1}^{n-1} \mu_{i-1} \dot{X}^i + \mu_{n-1} \underbrace{\dot{X}^n}_{= -\dot{a}_{n-1}\dot{X}^{n-1} - \dots - \dot{a}_0}$$

CQFD

Quelle est la matrice de la multiplication par X, dans E ?

$$X : E \to E$$
$$\dot{1} \mapsto \dot{X}$$
$$\dot{X} \mapsto \dot{X}^2$$
$$\text{-----}$$
$$\dot{X}^{n-1} \mapsto \dot{X}^n = -\dot{a}_0 - a_1\dot{X} - \dots - a_{n-1}\dot{X}^{n-1}$$

( $E = K[X]$-module $\forall \dot{Q} \in E$ $P\dot{Q}$ définit canoniquement par $P\dot{Q} = \dot{\widehat{PQ}}$ .
NB : $K[X] = K[X]$-module )

On connait les images de la base par la transformation X :

$$M = \begin{pmatrix} 0 & 0 & & & & -a_0 \\ 1 & 0 & & 0 & & -a_1 \\ 0 & 1 & \ddots & & & \vdots \\ & 0 & \ddots & & & \\ & & \ddots & \ddots & 0 & -a_{n-2} \\ & 0 & & 0 & 1 & -a_{n-1} \end{pmatrix}$$

On aura $K[X]/_{(P)} \underset{K[X]}{\simeq} (E, M) \simeq (K^n, M)$
(car $E \simeq K^n$)

M est la matrice "compagnon" du polynôme P.

Matrice caractéristique d'un endomorphisme

$E = K$-espace vectoriel de dimension n

$u \in End(E)$

Soit $(e_1, \dots, e_n)$ une base de E .

$$(K[X])^n \overset{\pi}{\twoheadrightarrow} E$$
$$(P_1, \dots, P_n) \longmapsto P_1 e_1 + \dots + P_n e_n$$

$\pi$ est surjective puisque tous les $P_i$ $(1 \leq i \leq n)$ peuvent être choisis constants

Cherchons le noyau de $\pi$ pour pouvoir faire paraître une matrice $M : (K[X])^n \longrightarrow (K[X])^n$ telle que la suite

$$(K[X])^n \xrightarrow{M} (K[X])^n \xrightarrow{\pi} E$$

soit exacte (en tant que $K[X]$-modules)

Th | Soit $A = (a_{ij})$ la matrice de $u$ dans la base $(e_i)_{1\leq i\leq n}$ et soit $M = A - XI$. C'est une matrice $n \times n$ à coefficients dans $K[X]$.

Alors la suite :

$$(K[X])^n \xrightarrow{M} (K[X])^n \xrightarrow{\pi} E \quad \text{est exacte}$$

Preuve : A montrer : $\operatorname{Im} M = \operatorname{Ker} \pi$

Nous allons introduire de nouvelles notations, commodes :

Si $E$ = e.v. sur $K$, on note $E[X] = \{ (v_0, v_1, \ldots, v_m, 0, \ldots) \doteq v_0 + v_1 X + \ldots + v_m X^m$ où $v_i \in E \}$

$E[X]$ ainsi défini est un $K[X]$-module grâce aux opérations :

$$\begin{cases} \sum_i v_i X^i + \sum_i w_i X^i = \sum_i (v_i + w_i) X^i \\ \left(\sum_i a_i X^i\right)\left(\sum_i v_i X^i\right) = \sum_i \left(\sum_k a_k v_{i-k}\right) X^i \end{cases}$$

Alors :

$$\forall \begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix} \in (K[X])^n \qquad \begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix} = \begin{pmatrix} \alpha_{10} \\ \vdots \\ \alpha_{n0} \end{pmatrix} + \begin{pmatrix} \alpha_{11} \\ \vdots \\ \alpha_{n1} \end{pmatrix} X + \cdots + \begin{pmatrix} \alpha_{1m} \\ \vdots \\ \alpha_{nm} \end{pmatrix} X^m$$

ce qui montre que tout "polynôme à coefficients vecteurs est aussi un vecteur à coefficients polynômes". Cette analogie permet ainsi d'affirmer que $E[X]$ est un $K[X]$-module libre.

En effet, si $(e_i)$ = $K$-base de $E$, $(e_i)$ = $K[X]$-base de $E[X]$

Traduisons notre suite en termes de $E[X]$ :

$$(K[X])^n \xrightarrow{u - XI} (K[X])^n \xrightarrow{\pi} E \qquad \text{devient :}$$

$$E[X] \xrightarrow{\tilde{u} - X id} E[X] \xrightarrow{\pi} E$$

$$v_0 + v_1 X + \dots + v_n X^n \longmapsto v_0 + u(v_1) + \dots + u^n(v_n)$$

?→ et où $\tilde{u}(v_0 + v_1 X + \dots + v_n X^n) = u(v_0) + u(v_1) X + \dots + u(v_n) X^n$

Montrons le théorème :

a) <u>$\mathfrak{Im}\, M \subset \mathrm{Ker}\, \pi$</u> ?

Faisons $\pi \circ M$, c.à.d $\pi \circ (\tilde{u} - X id)$

$(\tilde{u} - X id)(v_0 + v_1 X + \dots + v_n X^n) = u(v_0) + u(v_1) X + \dots + u(v_n) X^n - v_0 X$
$- \dots - v_n X^{n+1}$

car $X(v_0 + \dots + v_n X^n) = v_0 X + \dots + v_n X^{n+1}$.

Donc :

$\pi \circ (\tilde{u} - X id)(v_0 + \dots + v_n X^n) = u(v_0) + u^2(v_1) + \dots + u^{n+1}(v_n) - u(v_0)$
$- u^2(v_1) - \dots - u^{n+1}(v_n)$

$\pi \circ (\tilde{u} - X id)(v_0 + \dots + v_n X^n) = 0$

donc $\pi \circ M = 0 \Rightarrow \mathfrak{Im}\, M \subset \mathrm{Ker}\, \pi$ oui

b) <u>$\mathrm{Ker}\, \pi \subset \mathfrak{Im}\, M$</u> ?

$\mathrm{Ker}\, \pi \subset \mathfrak{Im}(\tilde{u} - X id)$ ?

$\pi(v_0 + \dots + v_n X^n) = 0 \Leftrightarrow v_0 + u(v_1) + \dots + u^n(v_n) = 0$

Alors :

$v_0 + v_1 X + \dots + v_n X^n = \cancel{v_0} + v_1 X + \dots + v_n X^n - \cancel{v_0} - u(v_1) - \dots - u^n(v_n)$
$= -(\tilde{u} - X id) v_1 - \dots - (\tilde{u}^n - X^n id) v_n$ (1)

[Posons $h = X id$, alors $u^n - h^n = (u - h)(u^{n-1} + u^{n-2} h + \dots + h^{n-1})$
est vrai si $u$ et $h$ commutent. C'est bien le cas ici puisque
$\tilde{u} \circ (X id) = (X id) \circ \tilde{u}$

Donc

$v_0 + \dots + v_n X^n = (\tilde{u} - X id)(\xi) \Rightarrow \mathrm{Ker}\, \pi \subset \mathfrak{Im}(\tilde{u} - X id)$

oui

**Def** | Soient $E$ un $K$-e.v. de dimension $n$, et soit $u \in \mathcal{L}(E)$. $P_1, \dots, P_n$ sont les polynômes élémentaires de $u$. Ils vérifient $P_1 | P_2 \dots P_{n-1} | P_n$.

$P_1 = \text{pgcd}(\text{mineurs d'ordre } 1 \text{ de la matrice carc. } M - XI)$

$P_1 \dots P_k = \text{pgcd}($ " " $k$ " " " $)$

$P_1 \dots P_n = $ polynôme caractéristique de $u$ $\chi_u(X)$.

**Pro** | $u, v \in \mathcal{L}(E)$ sont semblables ssi $P_i(u) = P_i(v)$ $\forall i \in [1,n]$ ($P_i$ moniques)

Exo : Calculer les polynômes élémentaires de ces endomorphismes :
$\begin{pmatrix} 1&0&0 \\ 1&1&0 \\ 0&0&1 \end{pmatrix}$ et $\begin{pmatrix} 1&0&0 \\ 1&1&0 \\ 0&1&1 \end{pmatrix}$.

## Intérêt d'une telle définition

$$E[X] \xrightarrow{\tilde{u} - X id} E[X] \xrightarrow{\pi} E$$

$$(e_i) \uparrow \sim \qquad (e_i) \uparrow \sim$$

$$(K[X])^n \xrightarrow{M - X id} (K[X])^n \xrightarrow{\pi} E \qquad (1)$$

chgt base ↑     chgt base ↑     ↖ $\Phi$ isomorphisme de $K[X]$-modules

$$(K[X])^n \xrightarrow[\begin{pmatrix} P_1 & & 0 \\ & \ddots & \\ 0 & & P_n \end{pmatrix}]{} (K[X])^n \xrightarrow{S} \bigoplus_{i=1}^n \left( K[X]/(P_i) \right) \qquad (2)$$

où $P_1 | \dots | P_n$

On peut trouver une telle matrice comme l'indique le théorème dans $\mathbb{Z}$ ?
La démonstration est la même et n'utilise que le fait que l'on a une division euclidienne dans $K[X]$ (anneau principal)

Alors : $(K[X])^n \longrightarrow (K[X])^n$

$$\begin{pmatrix} A_1 \\ \vdots \\ A_n \end{pmatrix} \longmapsto (P_1 A_1, P_2 A_2, \dots, P_n A_n) \simeq \bigoplus_{i=1}^n \left( K[X]/(P_i) \right)$$

c'est $\text{Im}(M - X id)$

Sur le diagramme de la page précédente, $\mathfrak{S}$ est défini par :

$$\mathfrak{S} : (K[X])^n \longrightarrow \bigoplus_{i=1}^{n} \left(K[X]/(P_i)\right)$$
$$(A_1, \dots, A_n) \longmapsto (\dot{A}_1, \dots, \dot{A}_n)$$

On a $\ker \mathfrak{S} = \operatorname{Im}(M - X\,id)$ : les suites (1) et (2) sont donc exactes.

Le "petit lemme des cinq" va permettre de conclure à l'existence d'un isomorphisme $\Phi$ de $K[X]$-module entre $E$ et $\bigoplus_{1}^{n} \left(K[X]/(P_i)\right)$

petit lemme des 5 : On se donne un diagramme commutatif de A-modules :

$$\begin{array}{ccccccc} M' & \xrightarrow{a} & M & \xrightarrow{p} & M'' & \longrightarrow & 0 \quad \text{exacte} \\ u\downarrow & & v\downarrow & & \downarrow w & & \\ N' & \xrightarrow{b} & N & \xrightarrow{q} & N'' & \longrightarrow & 0 \quad \text{exacte} \end{array}$$

$v \circ a = b \circ u$ (diagramme commutatif)

Alors, il existe un unique $w : M'' \to N''$ tel que le diagramme soit commutatif. De plus, si $u$ et $v$ sont des isomorphismes, alors $w$ l'est aussi

Preuve :

* On définit $w$ par : $\forall m'' \in M''$ $\exists m \,/\, p(m) = m''$

posons $w(m'') = q \circ v(m)$

Soit $m_1 \,/\, p(m_1) = m''$. Alors $m - m_1 \in \ker p = \operatorname{Im} a$, et donc $\exists m'$ tel que $m - m_1 = a(m')$.

A-t'on $q \circ v(m) = q \circ v(m_1)$ ?

On a $q \circ v(m - m_1) = q \circ v \circ a(m') = q \circ (b \circ u)(m') = 0$ car $q \circ b = \tilde{0}$. L'application $w$ est bien définie.

* $u$ et $v$ isomorphismes $\Rightarrow w = q \circ v$ est un isomorphisme. (facile)

Le lemme nous montre bien que

$$\bigoplus_{1}^{n} K[X]/(P_i) \xrightarrow{\Phi = \text{isomorphisme de } K[X]\text{-modules}} E$$

Remarques : 1) $\Phi$ est donc aussi un isomorphisme de K-e.v.

Donc $\dim_K E = \sum_{i=1}^{n} \dim_K K[X]/(P_i)$

$$\dim_K E = \sum_{i=1}^{n} \deg P_i$$

2)
Remarquons aussi que $P_i \neq 0$, car sinon $P_1 P_2 \dots P_n = \underbrace{\det(M - XI)}_{\neq 0} = 0$

3) Si $\forall i \in [1,n]$ $\deg P_i \neq 0$ alors $\sum_{i=1}^{n} \deg P_i = n \Rightarrow \deg P_i = 1$

Et $P_1 | \dots | P_n \Rightarrow P_i = (X-a)$

D'où $\chi_u(X) = (X-a)^n$

On sait que $K[X]/(X-a) \simeq \underbrace{(K, a)}_{\dim 1}$ puisque $Xe = ae$

d'où $E \simeq \bigoplus_{1}^{n} K[X]/(X-a) \Rightarrow u = a\, id$ est une homothétie.

Avec les notations de la définition précédente :

Z

| |
|---|
| Il existe un isomorphisme $\Phi$ de $K[X]$-modules $\bigoplus_{i=1}^{n} K[X]/(P_i) \xrightarrow[\Phi]{\sim} (E, u)$ |

L'intérêt d'un tel résultat est important :

## Réduction par blocs.

Si $P_i = X^{n_i} + a^i_{n-1} X^{n_i-1} + \dots + a^i_0$ $\quad n_i = \deg P_i$

Alors $(1, \dots, X^{n_i-1})$ est une base de $K[X]/(P_i)$ et la matrice compagnon de $P_i$ est

$$\begin{pmatrix} 0 & & & -a^i_0 \\ 1 & \ddots & & \vdots \\ \vdots & \ddots & 0 & \vdots \\ 0 & & 1 & -a^i_{n-1} \end{pmatrix}$$

$\forall u \in \mathcal{L}(E)$, il existe une base de $E$ telle que la matrice de $u$ soit diagonal~~isable~~ par blocs, chaque bloc étant la matrice compagnon d'un polynôme $P_i$.

$$\begin{pmatrix} \square & & & & \\ & \square & & 0 & \\ & & \square & & \\ & 0 & & \square & \\ & & & & \square \end{pmatrix}$$

$E \simeq \bigoplus_1^n K[X]/(P_i) \underset{\sim}{\to} (K^{\deg P_i}, u_i)$

d'où $E \simeq \bigoplus_1^n (K^{\deg P_i}, u_i) \simeq (K^n, v)$ où $v = \begin{pmatrix} u_1 & & 0 \\ 0 & \ddots & u_n \end{pmatrix}$

Mais $E \simeq (K^n, u)$

d'où $(K^n, u) \simeq (K^n, v) \Rightarrow u$ et $v$ semblables.

### Exemples :

1) Dans $\mathbb{R}^3$ $\quad u = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 2 & 0 \end{pmatrix}$

$$M - XI = \begin{pmatrix} 1-X & 0 & 0 \\ 2 & 1-X & 0 \\ 3 & 2 & -X \end{pmatrix} \qquad \begin{cases} P_1 = P_2 = 1 \\ P_3 = (1-X)^2 X = X^3 - 2X^2 + X \end{cases}$$

Le théorème nous donne :

$$(E, u) \xrightarrow[\sim]{\Phi^{-1}} \underbrace{\mathbb{R}[X]/\mathbb{R}[X] \times \mathbb{R}[X]/\mathbb{R}[X]}_{\text{él. neutre}} \times \mathbb{R}[X]/(X^3 - 2X^2 + X)$$

La matrice compagnon de $P_3$ est $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix} = v$

Ainsi $\underset{\mathbb{R}^3}{\overset{\shortparallel}{(E, u)}} \xrightarrow{\Phi^{-1}} (E, v) \Rightarrow u$ et $v$ semblables.

Dans cet exemple, on peut aller plus loin, en utilisant, par exemple, le théorème chinois :

**Rappel** : Théorème chinois dans $K[X]$

$$K[X]/_{(PQ)} \simeq K[X]/_{(P)} \times K[X]/_{(Q)} \quad \text{ssi} \quad \Delta(P,Q)=1$$

Dans notre exemple :

$$E \underset{K[X]\text{-mod.}}{\simeq} \mathbb{R}[X]/_{(X^3-2X^2+X)} = \mathbb{R}[X]/_{(X(1-X)^2)} \simeq \mathbb{R}[X]/_{(X)} \oplus \mathbb{R}[X]/_{((X-1)^2)}$$

Co | $u \in \mathcal{L}(E)$ et $\chi_u(X) = P_1 \dots P_n$ possède toutes ses racines dans $K$. Notons $P_i = \prod_j (X-\alpha_{ij})^{m_{ij}}$
Alors :

$$E \simeq \bigoplus_{i,j} K[X]/_{(X-\alpha_{ij})^{m_{ij}}}$$

D'où l'importance de la partie $K[X]/_{(X-\alpha)^m}$.

**Étude de $K[X]/_{(X-\alpha)^m}$**

C'est un e.v. sur $K$ ($K$ = corps) de base :

$$\underset{e_1}{\dot{1}}, \ \underset{e_2}{\dot{\overline{X-\alpha}}}, \dots, \underset{e_m}{\dot{\overline{(X-\alpha)}}^{m-1}}$$

On a :

$Xe_1 = X = (X-\alpha) + \alpha = e_2 + \alpha e_1$

$Xe_k = X(X-\alpha)^{k-1} = (X-\alpha)^k + \alpha(X-\alpha)^{k-1} \qquad \forall k \in [1, m[$

D'où :

$$\begin{cases} Xe_1 = \alpha e_1 + e_2 \\ \text{----} \\ Xe_k = \alpha e_k + e_{k+1} \quad \text{où } 1 \leq k < m \\ Xe_m = \alpha e_m \end{cases}$$

La matrice de la multiplication par $X$ dans $K[X]/_{(X-\alpha)^m}$, et dans la base $(e_k)_{1\leq k\leq m}$, est :

$$\begin{pmatrix} \alpha & & & & 0 \\ 1 & \alpha & & & \\ & 1 & \ddots & & \\ & & \ddots & \alpha & \\ 0 & & & 1 & \alpha \end{pmatrix}$$

c'est la matrice réduite de Jordan.

Le corollaire précédent peut s'énoncer ainsi : Si $\chi_u(X)$ a toutes ses racines dans $K$, il existe une base de $E$ dans laquelle la matrice de $u$ est diagonale par blocs de Jordan.

Exemple :

2) Dans $\mathbb{R}^3$, prenons $u = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 2 & 0 \end{pmatrix}$

$P_1 = P_2 = 1$ et $P_3 = X(X-1)^2$

On a vu que $E \simeq K[X]/_{(X-1)^2} \oplus K[X]/_{(X)}$ (th. Chinois)

La réduite de Jordan de cette matrice est donc :

$$\left(\begin{array}{cc|c} 1 & 0 & 0 \\ 1 & 1 & 0 \\ \hline 0 & 0 & 0 \end{array}\right)$$

## Polynôme minimal d'un endomorphisme

Def | $E = K$-e.v. de dimension $n$. Soit $u \in \mathcal{L}(E)$. On considère l'idéal $J$ de $K[X]$ défini par :

$$J = \{P \in K[X] \,/\, P(u) = 0 \in \mathrm{End}(E)\}$$

Alors $J = (P_m)$ où $P_m \doteq$ polynôme minimal de $u$

NB : $(E, u) = K[X]$-module. Alors $J = \{P \in K[X] \,/\, \forall v \in E \;\; P.v = 0\}$

Il s'agit du même $J$ que dans la définition puisque $P.v \doteq P(u)(v)$

Cette définition a un avantage sur la précédente : si $M$ est un module sur l'anneau $A$, on définit l'annulateur de $M$ par : $\text{Ann}\, M = \{a \in A \ / \ \forall m \in M \quad a.m = 0\}$.
Vu sous cet angle, le polynôme minimal de $u$ est le polynôme générateur de l'annulateur de $(E, u)$ :

$$(P_m) = \text{Ann}_{K[X]} E$$

Ex : $A = \mathbb{Z}$ $\quad M = \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}}$
$\text{Ann}\, M = 4\mathbb{Z} \subset \mathbb{Z}$
Plus généralement, si $M = \mathbb{Z}/_{d_1\mathbb{Z}} \times \dots \times \mathbb{Z}/_{d_r\mathbb{Z}}$ où $d_1 | \dots | d_r$, on a $\text{Ann}\, M = d_r\mathbb{Z}$

Théorème de Cayley-Hamilton.

Th | Soit $u \in \mathcal{L}(E)$ et $\chi_u(X)$ son polynôme caractéristique.
Alors $\chi_u(u) = \tilde{0}$

Preuve :
D'après le théorème fondamental :

$$E \underset{K[X]\text{-mod}}{\simeq} K[X]/_{(P_1)} \oplus \dots \oplus K[X]/_{(P_n)} \quad \text{où } P_1 | \dots | P_n$$

↑ Facile à obtenir

et $P_i$ moniques.
$\text{Ann}\, E = (P_n)$ où $P_n$ = polynôme minimal.

Or, nous avons : $P_n = \dfrac{P_1 \dots P_n}{P_1 \dots P_{n-1}} = \dfrac{\chi_u(X)}{\text{pgcd}(\text{min. d'ordre } n-1 \text{ de } (u - X\,id))}$

d'où $\chi_u = P_n (P_1 \dots P_{n-1}) \in (P_n) = \text{Ann}\, E \Rightarrow \chi_u \in \text{Ann}\, E$
donc $\chi_u(u) = \tilde{0}$.
CQFD

Z

## CNS pour que u soit diagonalisable

**Th** | $u \in \mathcal{L}(E)$ est diagonalisable ssi le polynôme minimal $P_n$ de $u$ :

1) possède toutes ses racines dans $K$
2) n'a que des racines simples.

### 1- méthode

($\Leftarrow$) Si $P_n(X) = (X-\alpha_1)\dots(X-\alpha_k)$ $\quad \alpha_i \neq \alpha_j$

on a : $E \simeq K[X]/_{(P_1)} \times \dots \times K[X]/_{(P_n)}$

où $P_j = \prod_{i \in I_j} (X-\alpha_i)$ où $I_j \subset [1,k]$

Le théorème chinois nous donne alors :

$$K[X]/_{(P_j)} \simeq \bigoplus_{i \in I_j} K[X]/_{(X-\alpha_i)}$$

donc $u$ est diagonalisable.

($\Rightarrow$)

*lemme* : Soient $Q_1, \dots, Q_r, R_1, \dots, R_s$ des polynômes irréductibles et tels que $i \neq j \Rightarrow R_i \neq R_j$ et $Q_i \neq Q_j$

Si $\bigoplus_{\substack{i=1 \\ k}}^{r} \left( K[X]/_{(Q_i^{a_k})} \right)^{m_{ik}} \simeq \bigoplus_{\substack{j=1 \\ l}}^{s} \left( K[X]/_{(R_j^{b_l})} \right)^{\boxed{n_{jl}}}$ ↑ attention ! ce n'est pas un exposant, c'est une répétition

Alors $r = s$, $Q_i = R_i$ et $m_{ik} = n_{jl}$ et $a_k = b_l$.

preuve du lemme : Si $R_1 \notin \{Q_1, \dots, Q_r\}$, comme $R_1$ est irréductible $\Delta(R_1, Q_j) = 1$

Donc $\forall j \in [1,n]$ $\quad \Delta(R_1, Q_j^{a}) = 1$

La multiplication par $R_1$ est une opération linéaire, inversi_
_ble dans le membre de gauche (cf (*)), alors qu'elle
ne l'est pas dans le membre de droite (cf (**)), d'où la
contradiction.

(*) $\Delta(P,Q) = 1$ et $E_1 = K[X]/_{(Q)}$ $\Rightarrow$ $P.$ est inversible dans $End(E_1)$.
En effet $\exists U, V \in K[X]$ / $UP + VQ = 1$
d'où, dans $E_1$ : $UP = 1$ $\Rightarrow$ $U.$ est l'inverse de $P.$ dans $End(E_1)$

(**) dans $K[X]/_{(R_1^b)}$ nous aurons $R_1 . \underbrace{(R_1)^{b-1}}_{\neq 0} = 0$

et donc $Ker(R_1 .) \neq 0 \Rightarrow R_1 . \neq$ isomorphisme.

Donc $\{R_1, \dots, R_s\} = \{Q_1, \dots, Q_s\}$
Reste à montrer que $K[X]/_{(R_1^a)}$ se repète un même nombre
de fois à gauche qu'à droite. Nous ne ferons pas la dém_
_onstration générale, mais nous verrons le mécanisme sur des
exemples :

1) $\underbrace{K[X]/_{(P^2)}}_{E_1} \not\simeq \underbrace{K[X]/_{(P)} \oplus K[X]/_{(P)}}_{E_2}$

car ils n'ont pas le même annulateur : $Ann\, E_1 = (P^2)$
$Ann\, E_2 = (P)$

2) $K[X]/_{(P)} \oplus K[X]/_{(P)} \oplus K[X]/_{(P^2)} \underbrace{\oplus -}_{\text{inversible par } P.} = K[X]/_{(P)} \oplus K[X]/_{(P^2)} \underbrace{\oplus -}_{\text{inversible par } P.}$

Noyau de l'application par P ?
A gauche : $\dim Ker(P.) = 3 \deg P$ (cf. $\circ$)
A droite : $\dim Ker(P.) = 2 \deg P$

△ $P_\circ : K[X]/_{(P^2)} \longrightarrow K[X]/_{(P^2)}$

$A$ / $\deg A < 2 \deg P$

$PA = RP^2 \Rightarrow A = RP \Rightarrow [\deg A < 2 \deg P \Rightarrow \deg R < \deg P]$

Donc $\mathrm{Ker}(P_\cdot)$ = e.v. de dimension $\deg P$.

3) $K[X]/_{(P)} \oplus K[X]/_{(P)} \oplus K[X]/_{(P^2)} \simeq K[X]/_{(P)} \oplus K[X]/_{(P^2)} \oplus K[X]/_{(P^2)}$

Noyau de l'application par $P^2$. ?

A gauche : $\dim \mathrm{Ker}(P^2_\cdot) = 4 \deg P$

A droite : $\dim \mathrm{Ker}(P^2_\cdot) = 5 \deg P$

( <u>Remarque</u> : analogie avec la question "Quels sont les nombres d'ordre $p$ dans $\mathbb{Z}/_{p^2\mathbb{Z}}$ où $p \in \mathcal{P}$ ?" On fait le diagramme $p\,\mathbb{Z}/_{p^2\mathbb{Z}} \hookrightarrow \mathbb{Z}/_{p^2\mathbb{Z}} \xrightarrow{p.} \mathbb{Z}/_{p^2\mathbb{Z}}$ )

Revenons à notre théorème :

($\Rightarrow$) Si 1) ou 2) faux, alors $u$ non diagonalisable ?

* $P_u$ n'a pas toutes ses racines dans $K$ :

Alors $u$ non diagonalisable

En effet, $u$ diagonalisable $\Rightarrow \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \Rightarrow \lambda_i \in K$.

* $P_u$ admet $\alpha$ comme racine multiple, dans $K$ :

$P_u = (X-\alpha)^a R$ où $R(\alpha) \neq 0$ et $a > 1$

Alors :

$$K[X]/_{(P_u)} \simeq \underbrace{K[X]/_{(X-\alpha)^a}}_{\text{facteur en } (X-\alpha)^a} \oplus K[X]/_{(R)}$$

↕ (cf. lemme précédent) — incompatibles

Or $u$ diagonalisable $\Rightarrow E \simeq \underbrace{\bigoplus_{i=1}^{n} K[X]/_{(X-\alpha_i)}}_{\text{facteurs en } (X-\alpha)}$

Donc u non diagonalisable

CQFD

2^e méthode

u diagonalisable $\Leftrightarrow$ $E = \bigoplus_{i=1}^{n} K[X]/(X-\alpha_i)$

(les $\alpha_i$ pas forcéments différents)

Quel est l'annulateur de E ?

$$\text{Ann}\, E = \bigcap_{i=1}^{n} (X-\alpha_i) \qquad (\text{ppcm des } (X-\alpha_i))$$

$$= \left(\prod_{j=1}^{k} (X-\alpha_{i_j})\right) \qquad \text{où } \{\alpha_{i_j}\} = \{\alpha_i\}$$

$$\text{et } \alpha_{i_1} < \alpha_{i_2} < \dots < \alpha_{i_k}$$

$\prod_{j=1}^{k} (X-\alpha_{i_j})$ est le polynôme minimal (par définition), et donc toutes ses racines sont simples.

CQFD

Application aux groupes linéaires finis.

Notons $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ où $p$ premier. C'est un exemple de corps fini.

Considérons $GL(n, \mathbb{F}_p)$ (matrices $n \times n$ à coefficients dans $\mathbb{F}_p$)

$$\# GL(n, \mathbb{F}_p) = (p^n - 1)(p^n - p)(p^n - p^2) \dots$$
$$\dots (p^n - p^{n-1})$$

ex : $n = 2$ $p = 2$, on obtient $GL(2, \mathbb{Z}/2\mathbb{Z})$ qui est un groupe à $(4-1)(4-2) = 6$ éléments

($GL(2, \mathbb{Z}/2\mathbb{Z}) \simeq \mathcal{S}_3$)

Problème : nombre de classes de conjugaisons

Rappel : $g, g' \in G$ conjugués $\Leftrightarrow \exists h \quad g' = hgh^{-1}$

On peut s'exprimer autrement, en disant que, si $G$ agit sur lui-même par automorphisme intérieur, alors la classe de conjugaison $C_g$ de $g$ est l'orbite de $g$ : $C_g = O_g$.

Dans $GL(V)$, $u$ et $u'$ sont conjugués $\Leftrightarrow$ $u$ et $u'$ semblables
$\Leftrightarrow \forall i \quad P_i(u) = P_i(u')$

Prenons $GL(2, \mathbb{F}_2)$ $\begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix}$

$$\begin{cases} P_1 P_2 = X^2 + \alpha X + 1 \\ \text{où } \alpha = 0 \text{ ou } 1 \end{cases}$$
(car $\det = \pm 1$ inversible dans $\mathbb{F}_2$) (dans $\mathbb{F}_2[X]$)

a) $P_1 P_2 = X^2 + 1 = (X+1)^2 \longrightarrow (X+1, X+1)$
$\searrow (1, (X+1)^2)$

b) $P_1 P_2 = X^2 + X + 1$ irréductible sur $\mathbb{F}_2[X]$ (sinon, il ~~posséd~~ serait divisible par un polynôme du 1^er^ degré et il posséderait une racine. Or il n'en possède pas : tester 0 et 1.) Il n'y a alors qu'une

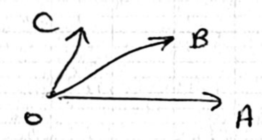
seule possibilité $(1, X^2+X+1)$

Il y a <u>3 classes de conjugaisons</u> dans ce groupe $GL(2, \mathbb{F}_2)$.

$$\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\} \quad \left\{\begin{pmatrix}1&0\\1&1\end{pmatrix} \; \begin{pmatrix}1&1\\0&1\end{pmatrix} \; \begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}$$

$$\left\{\begin{pmatrix}0&1\\1&1\end{pmatrix} \; \begin{pmatrix}1&1\\1&0\end{pmatrix}\right\}$$

$\mathfrak{S}_3 \simeq GL(2, \mathbb{F}_2)$ car $GL(2, \mathbb{F}_2)$ est l'ensemble des isomorphismes de $(\mathbb{F}_2)^2$ e.v. sur $\mathbb{F}_2$, qui possède 3 vecteurs non nuls :




D'où $GL(2, \mathbb{F}_2) \xrightarrow{\varphi} \mathfrak{S}_3$ homomorphisme surjectif
En fait, $\varphi$ = isomorphisme.

<u>Exercice</u> : Faire la même chose à $GL(3, \mathbb{F}_2)$ qui possède
(6 classes) 168 éléments. Et pour $GL(3, \mathbb{F}_q)$ ?

Solution : $GL(3, \mathbb{F}_q)$
$(P_1, P_2, P_3)$ tels que $P_1 | P_2 | P_3$ et $P_1 P_2 P_3 = \chi_u$
où $\chi_u(X) \in \{ X^3 + aX^2 + bX + c \text{ où } c \neq 0 \}$
Il y a $q^2(q-1)$ possibilités pour ce polynôme caractéristique.
La suite des degrés est :

$(P_1, P_2, \partial P_3)$
$(1, 1, 1)$ a)
$(0, 1, 2)$ b)
$(0, 0, 3)$ c)

a) $(X+a)^3, X+a, X+a)$ $a\neq 0$ $q-1$ possibilités
b) $(1, X+a, (X+a)(X+b))$ $(q-1)^2$ "
c) $(1, 1, X^3+aX^2+bX+c)$ $(q-1)q$ "
Le nombre de classes de conjugaisons est $(q^2-1)q$.

Rappels concernant les corps finis

Caractéristique d'un corps K

Def | L'ordre de 1 dans $(K,+)$ est appelé la caractéristique du corps K. On a : $\omega(1)$ = caractéristique de K.

Ainsi : Si $f : \mathbb{Z} \longrightarrow K$, $n \longmapsto n.1$

On a :

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & K \\ \downarrow & \nearrow & \\ \mathbb{Z}/p\mathbb{Z} & & \end{array}$$

$p\mathbb{Z} = \operatorname{Ker} f$

$\bar{f}$ = hom. injectif d'anneaux.

$\bar{f}(\mathbb{Z}/p\mathbb{Z})$ = sous-anneau de K
Si $p=0$, $\bar{f}(\mathbb{Z}) \subset K$ et donc K est infini.
Si $p\neq 0$, alors $\bar{f}(\mathbb{Z}/p\mathbb{Z})$ doit être intègre, et donc $\mathbb{Z}/p\mathbb{Z}$ aussi.
D'où p premier.

Pro | La caractéristique d'un corps est soit 0, soit un nombre premier.
Si caract$(K) = 0$, alors K est infini.

Preuve : cela a été fait ci-dessus. p désigne la caractéristique de K.

Pro | Soit $K$ un corps fini de caractéristique $p$. Alors $\mathbb{Z}/p\mathbb{Z} \hookrightarrow K$ (hom. de corps), et $K$ est un e.v. de dimension finie sur $\mathbb{Z}/p\mathbb{Z}$

Co | Soit $K$ un corps fini de caractéristique $p \in \mathcal{P}$. Alors $K \underset{e.v.}{\simeq} (\mathbb{Z}/p\mathbb{Z})^n$ et $\text{Card}\, K = p^n$

Preuve :
On définit $\bar{x}\, k = (x.1).k$ où $x.1 = \bar{f}(x)$, et l'on vérifie que ça marche.

Remarque : $K$ est un corps fini de cardinal $p^n$. Alors $K$ est le corps des racines du polynôme $X^{p^n} - X$ sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

$K = \{$racines du polynôme $X^{p^n} - X$ sur $\mathbb{F}_p\}$

En effet $K^* = K \setminus \{0\}$ est d'ordre $p^n - 1$. Donc :

$\forall x \in K^* \qquad x^{q-1} - 1 = 0 \qquad$ où $q = p^n$

donc : $\forall x \in K \qquad x^q - x = 0$

Posons $f(X) = X^q - X$. $f(X)$ possède $q$ racines distinctes dans $K$, à savoir tous les éléments de $K$ et $f$ se décompose en facteurs du premier degré ($K$ est commutatif)(*) dans $K[X]$.

Tout corps intermédiaire $L$ / $\mathbb{F}_p \subsetneq L \subsetneq K$, a moins de $q$ éléments et ne peut contenir les $q$ zéros distincts de $f$, donc $K$ est le corps des racines de $f$ sur $\mathbb{F}_p$.

Prenons par exemple :

$\text{Card}\, K = 4 \qquad K = \{0, 1, \alpha, \alpha^{-1}\}$ (caractéristique 2)

$(\mathbb{Z}/2\mathbb{Z})^2 \underset{e.v.}{\simeq} K$ et $f(X) = X^4 - X$

On a $\mathbb{Z}/2\mathbb{Z} \hookrightarrow K$, et $X^4 - X$ admet 2 racines dans $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Par contre $K$ contient toutes les racines de $f$.

(*) Tout corps fini est commutatif (Th. de      )

Exercice :

1) Si $K = \mathbb{F}_p$ , $\forall x \in \mathbb{F}_p$ $x^p = x \Rightarrow \forall x \in \mathbb{Z}$ $x^p \equiv x [p]$ ($p \in \mathcal{P}$). C'est le premier th. de Fermat.

2) Le produit des éléments non nuls de $\mathbb{F}_p$ est égal à $-1$ puisque, posant $a_q = 0$, on a :

$$X^{q-1} - 1 = \prod_{i=1}^{q-1} (X - a_i)$$

d'où $-1 = a_1 a_2 \dots a_{q-1}$

C'est le théorème de Wilson (d'ailleurs $\Leftrightarrow$ p premier)

Rappels concernant le corps des fractions d'un anneau commutatif intègre. (unitaire)

Soit $(A, +, \times)$ un anneau commutatif intègre. On se propose de plonger cet anneau A dans un corps K :

$$A \hookrightarrow K$$

c.à.d trouver K corps, tel qu'il existe un homomorphisme injectif d'anneaux de A vers K.

La démarche est la suivante :

$$K = \{(a,b) \in A \times (A \setminus \{0\})\} / \mathcal{R}$$

où $\mathcal{R}$ est la relation d'~ :

$$(a,b)\, \mathcal{R}\, (a',b') \Leftrightarrow ab' = ba'$$

On définit, sur $A \times A^*$ :

$$\begin{cases} (a,b) + (a',b') = (ab' + ba', bb') \\ (a,b) \times (a',b') = (aa', bb') \end{cases}$$

Ces deux relations sont compatibles avec $\mathcal{R}$. On peut donc définir ces lois sur le quotient

$(+, \times)$ définissent une structure d'anneau sur $A \times A^*$.

$(+, \times)$ " " de corps sur $K = A \times A^* / \mathcal{R}$

On vérifie que $A \hookrightarrow K$

$a \longmapsto \frac{a}{1}$

(où $\frac{a}{b} \doteq \dot{\overline{(a,b)}}$ )

<u>Remarque Importante</u> : $K$ = corps des fractions de $A$

$$\begin{array}{ccc} a & A & \xrightarrow[\varphi]{\text{anneaux}} L \text{ corps} \\ \downarrow & \downarrow & \nearrow \\ \frac{a}{1} & \text{corps } K & \bar{\varphi} \end{array}$$

$\exists ! \ \bar{\varphi}$ homomorphisme de corps, défini par : $\bar{\varphi}\left(\frac{a}{b}\right) = \varphi(a)(\varphi(b))^{-1}$

<u>Application</u> :

$\mathbb{Z} \hookrightarrow \mathbb{Q}$

$k[X] \hookrightarrow k(X) \doteq$ "corps des fractions rationnelles."

# Extensions de corps commutatif

<u>Def</u> : K est une extension du corps $k$ si $k \subset K$ et si K est un corps.
K est alors un $k$-espace vectoriel.

Soit $x \in K$ :
$k(x)$ = le plus petit corps qui contient $k$ et $x$.
$k[x]$ = le plus petit anneau qui contient $k$ et $x$

On a $k(x) \supset k[x]$ mais pas forcément l'égalité.

## Éléments transcendants et éléments algébriques sur $k$.

Soit $x \in K$. On peut définir :

$$\begin{array}{ccc} k[X] & \xrightarrow{\varphi} & K \\ P & \longmapsto & P(x) = \sum a_i x^i \end{array} \quad \text{hom. d'anneaux}$$

C'est même un homomorphisme d'e.v. sur $k$.
Manifestement $\operatorname{Im}\varphi = k[x]$. De 2 choses l'une :

1°/ <u>$\varphi$ est injective : éléments transcendants sur $k$</u>

$\operatorname{Ker}\varphi = \{0\}$ et d'après les rappels du chapitre précédent, on a :

$$k[X] \overset{\varphi}{\hookrightarrow} K \quad \text{où } \operatorname{Im}\varphi = k[x]$$

$$k[X] \hookrightarrow k(X) \nearrow K$$

$\psi$ homomorphisme injectif de corps

$$\psi\left(\frac{P}{Q}\right) = \varphi(P)\,[\varphi(Q)]^{-1}$$

où $k(X)$ est le corps des fractions de $k[X]$. Ainsi, nous pouvons considérer $k(X)$ comme un sous-corps de $K$

**Def** | Si $\varphi$ est injective, $x$ est dit "transcendant sur $k$".

L'expression de $\psi$ permet d'énoncer :

**Pro** | $x \in K$ est transcendant sur $k$ ssi :

$$\frac{P(x)}{Q(x)} = \frac{P'(x)}{Q'(x)} \in K \Rightarrow \frac{P(X)}{Q(X)} = \frac{P'(X)}{Q'(X)} \in k(X)$$

où $P, Q, P', Q' \in k[X]$

<u>Remarque</u> :

Le nombre $\pi$ est transcendant sur $\mathbb{Q}$ (dem. 1852 Lindeman)

Par conséquent $\forall P \in \mathbb{Q}[X] \quad P(\pi) \neq \frac{1}{1+\pi^2}$

<u>Exo</u> : Montrer qu'alors $k[X] \underset{\text{anneaux}}{\simeq} k[x]$ et que l'on a : $k(X) \underset{\text{corps}}{\simeq} k(x)$
(utiliser $\varphi$ et $\psi$)

## 2°/ Éléments algébriques sur $k$

Si $\varphi : k[X] \to K$ n'est pas injective, on pose $\ker \varphi = (P)$ où $P = X^n + \dots + a_1 X + a_0$
(Car $k[X]$ principal)

**Pro** | Si $\varphi : k[X] \to K$ n'est pas injective, on a $k[X]/(P) \overset{\bar{\varphi}}{\hookrightarrow} K$ où $\bar{\varphi}$ = homomorphisme d'anneaux et où $P$ est irréductible.

Preuve :

__1-méthode__ : On a :

$$\begin{array}{ccc} k[X] & \xrightarrow{\varphi} & K \\ \downarrow & & \uparrow \\ k[X]/_{(P)} & \xrightarrow{\bar{\varphi}} & k[x] = \mathrm{Im}\,\varphi \end{array}$$

$\bar{\varphi}$ = isomorphisme d'anneaux. $\mathrm{Im}\,\varphi$ est un anneau intègre, donc $k[X]/_{(P)}$, qui est un anneau unitaire, est aussi intègre.
Alors $k[X]/_{(P)}$ est un corps (lemme 1)
Le lemme 2 permet d'affirmer que $P$ est irréductible.
CQFD

__lemme 1__ : $k[X]/_{(P)} = E$ anneau unitaire intègre $\Rightarrow$ $E$ = corps.
Preuve :
Soit $u : E \to E$ $\quad$ ($E$ = e.v. sur $k$)
$\quad \dot{X} \mapsto \dot{Q}\dot{X}$ où $\dot{Q} \neq \dot{0}$
$u$ est linéaire car $u(\dot{X} + \lambda \dot{Y}) = u(\dot{X}) + \lambda u(\dot{Y})$ $\quad \forall \dot{X}, \dot{Y} \in E$
$\mathrm{Ker}\, u = \{ \dot{X} / \dot{Q}\dot{X} = \dot{0} \}$ $\quad \forall \lambda \in k$
Mais $\dot{Q}\dot{X} = \dot{0} \Rightarrow \dot{X} = \dot{0}$, donc $u$ bijective. cqfd

__lemme 2__ : $k[X]/_{(P)}$ = corps $\Leftrightarrow$ $P$ irréductible dans $k[X]$
Preuve :
* $P = QR \Rightarrow \dot{Q}.\dot{R} = \dot{P} = \dot{0}$ et $\dot{Q} \neq \dot{0}$, $\dot{R} \neq \dot{0}$
* Si $P$ est irréductible, soit $\dot{A} \neq \dot{0}$. Alors $\Delta(P, A) = 1$ donc $\exists U, V$ / $\dot{U}\dot{P} + \dot{V}\dot{A} = \dot{1} \Leftrightarrow \dot{V}\dot{A} = \dot{1}$ donc $k[X]/_{(P)}$ est un corps.
cqfd

__2-méthode__ :

$$\begin{array}{ccc} k[X] & \xrightarrow{\varphi} & K \\ \downarrow & \nearrow_{\bar{\varphi}} & \\ k[X]/_{(P)} & & \end{array}$$

Si $P$ était réductible : $P = QR$ $\begin{cases} \deg R > 1 \\ \deg Q > 1 \end{cases}$

d'où : $\varphi(Q)\varphi(R) = 0$ et $\varphi(Q) \neq 0$, $\varphi(R) \neq 0$ ce qui contredit l'hypothèse " $K$ = corps ".

oui.

Def | Soit $x \in K$ tel que $\ker \varphi = (P)$. Alors $x$ est "un élément algébrique sur $k$", et $P$ est appelé le "polynôme minimal de $x$".

$P(x) = 0$ et $P$ irréductible.

Pro | $x$ algébrique sur $k \iff \exists P \neq 0$ $P \in k[X]$ / $P(x) = 0$

Pro | $x$ algébrique sur $k \Rightarrow k[x] = k(x)$

En effet, $\bar{\varphi} : k[X]/_{(P)} \longrightarrow k[x] = \mathrm{Im}\,\varphi$ est un isomorphisme d'anneaux, et $k[X]/_{(P)}$ est un corps.
Donc $k[x]$ est un corps, et c'est le p. petit contenant $k$ et $x$ :
$k[x] = k(x)$

<u>Exemples</u> : $\sqrt{2}$, $i + \sqrt{2}$, $i\sqrt{3}$ sont-ils algébriques sur $\mathbb{Q}$ ?
Sol :
$\sqrt{2}$ est racine de $X^2 - 2$ oui
$(i+\sqrt{2})^2 = 2i\sqrt{2} + 1 \Rightarrow ((i+\sqrt{2})^2 - 1)^2 = -8$ oui
$i\sqrt{3}$ est racine de $X^2 + 3 = 0$.

(NB : non algébrique = transcendant)

Tableau récapitulatif :

$x \in K \quad k \subset K$

| $x$ transcendant sur $k$ | $x$ algébrique sur $k$ |
|---|---|
| $\frac{P(x)}{Q(x)} = 0 \in K \Rightarrow \frac{P}{Q} = 0 \in k(X)$ | $\exists P \neq 0$ tel que $P(x) = 0$ |
| $\mathrm{Im}\,\varphi = k[x]$ | $\mathrm{Im}\,\varphi = k[x]$ |
| $k[X] \overset{\varphi}{\hookrightarrow} K$ ; $k[X] \hookrightarrow k(X)$ ; $k(X) \overset{\psi \text{ corps}}{\hookrightarrow} K$ | $k[X] \overset{\varphi}{\longrightarrow} K$ ; $k[X] \to k[X]/(P)$ ; $k[X]/(P) \overset{\bar\varphi \text{ corps}}{\hookrightarrow} K$ |
| $k[x] \underset{\text{ann.}}{\simeq} k[X]$ | $k[x] = k(x)$ |
| $k(x) \underset{\text{corps}}{\simeq} k(X)$ (ev) | $k(x) \underset{\text{corps (ev) sur } k}{\simeq} k[X]/(P)$ |

3°/ Propriétés

> **Th** | $x \in K$ et $k \subset K$
> $x$ est algébrique sur $k$ ssi $[k[x] : k] < \infty$ (en fait $k(x)$)

On note $[K : k] = \dim_k K$ où $K$ est une extension de $k$.

$(\Rightarrow)$ $k[x] \simeq k[X]/(P)$ d'où $[k[x] : k] = \deg P$

$(\Leftarrow)$ Si $\dim_k k(x) = n$ $\quad k(x) \subset K$

Alors $1, x, \dots, x^n \in k(x)$ sont liés, et donc :

$$\exists (a_0, \dots, a_n) \neq (0, \dots, 0) \ / \ \sum_{i=0}^{n} a_i x^i = 0$$

CQFD

Definition : On dit que $K$ est une extension algébrique de $k$

si tout élément de $K$ est algébrique sur $k$.
(c.à.d si $\forall x \in K \ \exists P \in k[X] / \ P(x) = 0$)
Si l'extension $K$ n'est pas algébrique, elle est dite transcen_
_dante

Th | L'ensemble des nombres algébriques sur $\mathbb{Q}$ (ou plus généralement, sur un corps dénombrable) est dénombrable.

$\mathbb{Q}$ dénombrable, donc $P(x) = a_{i_n} x^n + \dots + a_{i_0}$ est l'écriture des polynômes sur $\mathbb{Q}$. On numérote ces polynômes par :
$n + \sum i_j = 0, 1, \dots$ où $n = \deg P$

Exo : Montrer que $\mathbb{Q}$ est dénombrable. Montrer que $\mathbb{R}$ ne l'est pas (Cantor)

Th | $[K:k] < \infty \Rightarrow K$ est une extension algébrique de $k$
(extension "finie")

En effet, si $x \in K$ $\quad k \subset k[x] \subset K$
$\forall x \quad \dim_k k[x] \leq \dim_k K < \infty \Rightarrow x$ algébrique.

**Lemme** $k \subset K \subset L$
Alors $[L:k] = [L:K] \times [K:k]$ (dans $\overline{\mathbb{N}}$)

Preuve : On suppose $[L:K] < \infty$ et $[K:k] < \infty$, sinon

c'est trivial.

Soient $(x_1, \dots, x_m)$ une base $K$ (sur $k$)

et $(y_1, \dots, y_n)$ une base de $L$ (sur $K$)

$\forall \ell \in L \quad \exists (b_1, \dots, b_n) \in K^n \quad \ell = \sum_1^n b_i y_i$

et $b_i = \sum_{j=1}^{m} a_{ij} x_j$

d'où $\ell = \sum_{i,j} a_{ij} (x_j y_i)$, et $(x_j y_i)_{i,j}$ est un système généra_teur de $L$ sur $k$. Montrons que ce système est libre :

$\begin{cases} \sum_{i,j} \alpha_{ij} (x_j y_i) = 0 \\ \alpha_{ij} \in k \end{cases} \Rightarrow \sum_i \underbrace{\left( \sum_j \alpha_{ij} x_j \right)}_{\in K} y_i = 0$

$\Rightarrow \begin{cases} \sum_j \alpha_{ij} x_j = 0 \\ \forall i \end{cases} \Rightarrow \alpha_{ij} = 0 \quad \forall i, j.$ CQFD

Th | Soit $k \subset K$ et $x, y \in K$.
$\left.\begin{array}{l} x \text{ algébrique sur } k \\ y \text{ algébrique sur } k(x) \end{array}\right\} \Rightarrow y$ algébrique sur $k$

Preuve : On a $\begin{cases} [k(x) : k] < \infty \\ [k(x)(y) : k(x)] < \infty \end{cases}$

~~d'où $[k(x)(y) : k(x)] \times [k(x) : k] =$~~

d'où $[k(x)(y) : k] = [k(x,y) : k(x)] \times [k(x) : k] < \infty$ (cf. lemme)

On a $k(xy) = k(x)(y)$, bien sûr.

Mais $k(y) \subset k(xy)$, donc $[k(y) : k] \leq [k(x,y) : k] < \infty$

C.à.d $y$ algébrique sur $k$

CQFD

Th | L'ensemble des nombres de $K$ algébriques sur $k$ est un corps.

Preuve : Si $x$ et $y$ sont algébriques sur $k$, alors $y$ est algé_
_brique sur $k(x)$, et donc $[k(x,y) : k] < \infty$

Alors $\begin{cases} k(x-y) \subset k(x,y) \\ k(xy^{-1}) \subset k(x,y) \end{cases}$

d'où $\begin{cases} [k(x-y) : k] < \infty \Rightarrow x-y \text{ algébrique sur } k \\ [k(xy^{-1}) : k] < \infty \Rightarrow xy^{-1} \text{ algébrique sur } k \end{cases}$

4°/ Théorème de Liouville

On dira qu'un élément est algébrique si c'est un élément de $\mathbb{C}$ algébrique sur $\mathbb{Q}$ :

$x$ algébrique $\Leftrightarrow$ $x \in \mathbb{C}$ et $\exists P \in \mathbb{Z}[X] \ / \ P(x) = 0$

Th | $x \in \mathbb{R}$ est transcendant si la condition suivante est vérifiée :

$\exists K \in \mathbb{R}_+ \quad \forall n \in \mathbb{N} \quad \exists \frac{p}{q} \in \mathbb{Q} \quad \left|\frac{p}{q} - x\right| \leq \frac{K}{q^n}$

Exemple : $x = \sum_{n=1}^{\infty} \frac{1}{10^{n!}} = 0,110001 0 \ldots 010 \ldots$

vérifie cette condition : Posons $x_n = \sum_{i=1}^{n} \frac{1}{10^{i!}} \in \mathbb{Q}$

Alors $|x_n - x| < \frac{2}{10^{(n+1)!}}$ car $10^{(n+1)!} = (10^{n!})^{n+1} > (10^{n!})^n$

Preuve : Supposons que $x$ soit algébrique sur $\mathbb{Q}$, notons $f(X) \in \mathbb{Q}[X]$ son polynôme minimal. On peut choisir $f \in \mathbb{Z}[X]$.

$\deg f = r$

Soit $\frac{p}{q} \in \mathbb{Q}$ $\exists A$ $\left|\frac{p}{q} - x\right| < A \Rightarrow f\left(\frac{p}{q}\right) \neq 0$ vrai car les zéros de $f$ sont isolés.

$f(X) = a_n X^n + \ldots + a_0$ $\quad f\left(\frac{p}{q}\right) = \frac{a_n p^r + a_{n-1} p^{r-1} q + \ldots + a_0 q^r}{q^r}$

(prenons $q \geq 2$)

d'où $\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^n}$ (1)

D'autre part $\left|f\left(\frac{p}{q}\right)\right| = \left|f\left(\frac{p}{q}\right) - f(x)\right| = |f'(c)| \left|\frac{p}{q} - x\right| \leq M \left|\frac{p}{q} - x\right|$

où $M \geq \sup_{c \in [x-A, x+A]} |f'(c)|$ (2)

Si le nombre $x$ était de Liouville, on aurait :

$$\forall n \in \mathbb{N} \quad \frac{1}{q^n} \leq \left|f\left(\frac{p}{q}\right)\right| \leq M \left|\frac{p}{q} - x\right| \leq M \frac{K}{q^n}$$

d'où $\frac{1}{q^n} = 0$ (on prend $q \geq 2$), ce qui est absurde.

CQFD

Critère d'Eiseinstein (polynômes irréductibles sur $\mathbb{Q}$)

1°/ Rappel Def | A anneau commutatif $a \neq 0$ est dit irréductible si $a \notin A^*$ et si les seuls diviseurs de $a$ sont les $u \in A^*$ et les $au$ où $u \in A^*$.

Def | A anneau ; $a \in A$ est dit irréductible si

$$\begin{cases} a = bc \Rightarrow b \text{ ou } c \in A^* \\ \text{et } a \notin A^* \end{cases}$$

(NB : $A^*$ = ens. des éléments inversibles de A)

Si K est un corps, on sait que les seuls éléments inversibles de $K[X]$ sont les constantes. Dans ce cas particulier :

$P \in K[X]$ irréductible $\Leftrightarrow$ P ne possède pas d'autres diviseurs que les constantes ou lui-même, à une cte près.

En effet, $P = QR \Rightarrow Q$ ou $R$ de degré 0

$\Rightarrow Q = a \in K$ et $R = \frac{1}{a} P$.

Par exemple, si $K = \mathbb{R}$ :

$P \in \mathbb{R}[X]$ irréductible $\Leftrightarrow \{P = QR \Rightarrow \deg Q = 0$ ou $\deg R = 0\}$.

Exo : Montrer que dans $\mathbb{R}[X]$, les polynômes de degré 2 ou 3 irréductibles sont ceux qui n'admettent pas de racines dans $\mathbb{R}$.

## 2°/ Critère d'Eisenstein

**Pro** Si $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$ vérifie les conditions :

1) $a_n \not\equiv 0 \ [p]$
2) $a_i \equiv 0 \ [p]$ $\quad p \in \mathcal{P} \quad 0 \leq i < n$
3) $a_0 \not\equiv 0 \ [p^2]$

Alors $P$ est irréductible dans $\mathbb{Q}[X]$.

Démonstration :

a) $P$ est irréductible dans $\mathbb{Z}[X]$.

Supposons que $P = QR$ où $\begin{cases} Q = b_r X^r + \dots + b_0 \\ R = c_{n-r} X^{n-r} + \dots + c_0 \end{cases}$

On a $a_0 = b_0 c_0$

$p | a_0$ et $p^2 \nmid a_0 \Rightarrow p | c_0$ et $p \nmid b_0$ (par exemple)

Ainsi $c_0 \equiv 0 \ [p]$ et $b_0 \not\equiv 0 \ [p]$

Soit $m = \operatorname{Inf}\{ i \in \mathbb{N} \ / \ c_i \not\equiv 0 \ [p] \}$. On a $c_m \not\equiv 0 \ [p]$

Mais :

$$a_m = \underbrace{b_0 c_m}_{\not\equiv 0 [p]} + \underbrace{b_1 c_{m-1} + \dots + \begin{cases} b_m c_0 \text{ si } r > m \\ b_r c_{m-r} \text{ si } r \leq m \end{cases}}_{\text{divisible par } p}$$

Donc $a_m \not\equiv 0 \ [p] \Rightarrow m = n$

Mais $m \leq n - r \Rightarrow 0 \leq -r \Rightarrow r = 0 \Rightarrow \deg R = n$

donc $P(X) = a\, R(X)$ où $R(X) \in \mathbb{Z}[X]$. Montrons que $a = \pm 1$.

On remarque que $P(X) = \delta\,(a'_n x^n + \dots + a'_0)$ où $\delta = \Delta(a_0, a_1, \dots, a_n)$ et que l'irréductibilité de $P$ (dans $\mathbb{Q}$) est celle de $P' = a'_n X^n + \dots + a'_0$ dans $\mathbb{Q}[X]$. Le raisonnement précédent est valable pour $P'$ car les conditions 1) 2) et 3) sont vérifiées pour $P'$. Alors :

$a_i = a\, c_i \quad i \in [0, n] \Rightarrow a = \pm 1 \Rightarrow P'(X) = \pm R(X)$.

Donc $P'$ est irréductible dans $\mathbb{Z}[X]$

b) P est irréductible dans $\mathbb{Q}[X]$.
(C'est un résultat classique).

Lemme : $\forall P \in \mathbb{Z}[X]$
P irréductible dans $\mathbb{Z}[X] \Rightarrow$ P irréductible dans $\mathbb{Q}[X]$

Preuve : Si $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$, on le décompose en $P = d P^*$ où $d = \Delta(a_i)$ et $P^* =$ polynôme primitif (c-à-d dont tous les coefficients sont premiers entre eux).
On démontre que cette décomposition est unique (au signe près)
Cela étant posé :
Si P est irréductible dans $\mathbb{Z}[X]$, alors il est primitif (cf. (*)) et si $P = QR$ dans $\mathbb{Q}[X]$ on a $NP = n_1 Q_1 \cdot m_1 R_1$ après avoir réduit au même dénominateur et après avoir décomposé en $Q_1, R_1$ primitifs.
De l'égalité $NP = n_1 m_1 Q_1 R_1$ on tire $P = \pm Q_1 R_1$, dans $\mathbb{Z}[X]$. Par hypothèse cela implique que

$Q_1$ ou $R_1 = 1$ par exemple $Q_1 = 1$

d'où $\deg Q = \deg Q_1 = 0$
P est irréductible dans $\mathbb{Q}[X]$.

CQFD

Remarque (*) :
$2(X+1)$ n'est pas irréductible dans $\mathbb{Z}[X]$ puisque $X+1$ et $2$ ne sont pas inversibles dans $\mathbb{Z}[X]$ !

Adjonction symbolique - Corps de rupture d'un polynôme. Corps des racines

## 1°/ Définitions : corps de rupture

Étant donné un corps $k$ et un polynôme $P$ irréductible de $k[X]$, de degré $> 1$, peut-on trouver une extension $K$ de $k$ dans laquelle $P$ possède au moins une racine ?

### a) Corps de rupture

$k$ = corps, $P \in k[X]$ irréductible sur $k$, monique.

Alors $k[X]/_{(P)}$ est un corps. Soit $\pi$ l'épimorphisme canonique $\pi : k[X] \longrightarrow k[X]/_{(P)}$. La restriction de $\pi$ au corps $k$ est injective car :

$$\pi(a) = \pi(b) \Rightarrow \pi(a-b) = 0 \Leftrightarrow a-b \in (P)$$

d'où $a = b$ car $\deg(a-b) = 0$

D'où $k \overset{\pi}{\hookrightarrow} k[X]/_{(P)}$ et $k[X]/_{(P)}$ peut être considéré comme un sur-corps de $k$.

Posons $\pi(X) = \alpha$.

$\forall Q \in k[X] \quad \pi(Q) = Q(\alpha)$

$Q(\alpha)$ est une expression polynomiale en $\alpha$, donc $k[X]/_{(P)} \subset k[\alpha]$

Comme $\operatorname{Ker}\pi = (P)$ $\quad \pi(P) = P(\alpha) = 0$ donc $\alpha$ est algébrique sur $k$.

$\alpha \in k[X]/_{(P)} \Rightarrow k(\alpha) = k[\alpha] \subset k[X]/_{(P)}$

Finalement $k(\alpha) = k[X]/_{(P)}$

**Th** Soit $k$ un corps et $P$ un polynôme non nul de degré $> 1$, irréductible sur $k$. Alors il existe une extension algébrique $K$ de $k$ dans laquelle $P$ a une racine.

Ce procédé de construction de surcorps de $k$ s'appelle "adjonction symbolique".

b) Exemples

① L'extension simple

$$\mathbb{Q}[X]/_{(X^3-2)} \simeq \mathbb{Q}(\alpha)$$

est un corps de rupture du polynôme $X^3-2$ irréductible sur $\mathbb{Q}$.
$\mathbb{Q}(\alpha)$ est un $\mathbb{Q}$-ev de dimension 3, de base $\{1, \alpha, \alpha^2\}$
Sur $\mathbb{Q}(\alpha)$, on a la décomposition :

$$X^3 - 2 = (X-\alpha)(X^2+\alpha X+\alpha^2)$$

On montre (cf Querré p 91) que le polynôme $X^2+\alpha X+\alpha^2$ est irréductible sur $\mathbb{Q}(\alpha)$ et donc que dans le corps de rupture $\mathbb{Q}(\alpha)$, le polynôme $X^3-2$ n'est pas totalement décomposé en facteurs linéaires.

② Nombres complexes :
$X^2+1$ irréductible sur $\mathbb{R}$

$$\pi : \mathbb{R}[X] \rightarrow \mathbb{R}[X]/_{(X^2+1)}$$
$$X \longmapsto i \text{ (notation)}$$

Donc $\mathbb{R}(i) \simeq \mathbb{R}[X]/_{(X^2+1)}$
On pose $\mathbb{C} = \mathbb{R}(i)$. C'est un $\mathbb{R}$-espace vectoriel de dim 2 sur $\mathbb{R}$, et de base $\{1, i\}$
Dans $\mathbb{C}$ : $X^2+1 = (X-i)(X+i)$ car $i^2 = -1$.

Remarque : d'après le th. de d'Alembert, tout polynôme de $\mathbb{C}[X]$ de degré $\geq 1$ admet au moins une racine.
On ne pourra donc construire aucune extension algébrique simple du corps des nbres complexes.

$$\boxed{\mathbb{C} = \mathbb{R}[X]/_{(X^2+1)}}$$

## 2°/ Corps des racines d'un polynôme.

**Th** | Soit P un polynôme de degré $n \geqslant 1$ sur un corps K. Alors il existe une extension E finie de K, de degré au plus $n!$ dans laquelle P possède n racines.

Au 1°/, on a montré l'existence de l'extension simple $E_0$ du corps K dans laquelle P a une racine $\alpha_1$

$$[E_0 : K] \leq \deg f = n$$

Soit E $P(X) = (X - \alpha_1)\, P_1(X)$ dans $E_0[X]$

$\deg P_1 = n - 1$.

Il existe $E_1$ où $P_1$ a une racine. Dans $E_1[X]$ :

$$P(X) = (X - \alpha_1)(X - \alpha_2)\, P_2(X) \qquad \deg P_2 = n - 2$$

et $[E_1 ; E_0] \leqslant n - 1$

On construit donc une suite croissante d'extensions

$$E_0 \subset E_1 \subset \cdots \subset E_{n-1}$$

tel que $[E_i ; E_{i-1}] \leqslant n - i$

D'où $[E_{n-1} ; K] = \prod [E_i ; E_{i-1}] \leqslant 1.2. \ldots . n = n!$

**Def** | L'extension finie E, définie ci-dessus, s'appelle "corps de factorisation de P".

C'est donc un corps dans lequel le polynôme se factorise en facteurs du premier degré. C'est une extension finie de K.

**Def** | On appelle "corps des racines" (ou "corps de factorisation totale") d'un polynome P sur un corps K une extension $\Sigma$ de K tel que 1) $\Sigma$ est un corps de factorisation de P
2) $\Sigma$ est minimal dans l'ensemble

des corps de factorisation de $P$, c.à.d que sur tout corps intermédiaire $F$ ($K \subset F \subset \Sigma$) $P$ ne se décompose pas en facteurs du 1° degré.

Exemple 1) $X^3-2$ irréductible sur $\mathbb{Q}$.
$\alpha$ = racine de $X^3-2$. $\mathbb{Q}(\alpha)$ n'est pas un corps de factorisation de $X^3-2$ (déjà vu).
Dans $\mathbb{Q}(\alpha, j)$ : $X^3-2 = (X-\alpha)(X-j\alpha)(X-j^2\alpha)$
Ainsi $\mathbb{Q}(\alpha,j)$ est un corps de factorisation de $X^3-2$, et l'on a $[\mathbb{Q}(\alpha,j) ; \mathbb{Q}] = 6$
Montrons que $\mathbb{Q}(\alpha,j)$ est le corps des racines de $X^3-2$ : Si $F$ = corps tel que $\mathbb{Q} \subset F \subset \mathbb{Q}(\alpha,j)$, et $F$ = corps de factorisation de $P$, alors $\alpha, j \in F \Rightarrow \mathbb{Q}(\alpha,j) \subset F \Rightarrow \mathbb{Q}(\alpha,j) = F$.
CQFD

Exemple 2) Corps des racines de $X^4-3$ ?
Soit $\alpha = \sqrt[4]{3}$ une racine de $X^4-3$. C'est un polynôme irréductible sur $\mathbb{Q}$.

$$[\mathbb{Q}(\alpha) ; \mathbb{Q}] = 4$$

et $X^4-3 = (X-\alpha)(X^3+\alpha X^2+\alpha^2 X+\alpha^3)$
Les autres racines (complexes) de $X^4-3$ sont :

$$-\alpha \quad i\alpha \quad -i\alpha$$

Le corps des racines de $X^4-3$ est $\mathbb{Q}(\alpha, -\alpha, i\alpha, -i\alpha)$
c.à.d $\mathbb{Q}(\alpha, i\alpha) = \mathbb{Q}(\alpha, i)$. Son degré est :

$$[\mathbb{Q}(\alpha,i) ; \mathbb{Q}(\alpha)] \times [\mathbb{Q}(\alpha) ; \mathbb{Q}] = 2 \times 4 = 8$$

puisque $X^2+1$ est le polynôme minimal de $i$ dans $\mathbb{Q}(\alpha)$.

Unicité du corps des racines d'un polynôme

## 1°/ Enoncé du théorème d'Unicité

Th | Soit $\varphi : K \to K'$ isomorphisme de corps.
$f \in K[X]$ et $f' = \varphi(f) \in K'[X]$
$\Sigma$ et $\Sigma'$ sont resp. des corps de racines de $f$ et $f'$
Alors $\exists\ \alpha : \Sigma \to \Sigma'$ isomorphisme de corps prolongeant $\varphi$

$$\begin{array}{ccc} K & \xrightarrow[\sim]{\varphi} & K' \\ \downarrow & & \downarrow \\ \Sigma & \xrightarrow[\sim]{\alpha} & \Sigma' \end{array}$$

Preuve : Récurrence sur le degré $n = [\Sigma ; K]$

* $n = 1$ trivial
* Supposons le th. vrai pour tout corps de racines de degré inférieur strictement à $n$, sur un corps $K$.

Soit $n > 1$. Toutes les racines de $f$ ne sont pas dans $K$, et $f$ possède au moins un facteur irréductible $p$ de degré $d > 1$. Soit $\alpha$ une racine de $p$ appartenant à $\Sigma$.
Soit $p'$ l'homologue de $p$ par $\varphi$ :

$$f = p p_1 \Rightarrow f' = \varphi(p)\varphi(p_1)$$

$\Sigma'$ contient une racine $\alpha'$ de $p'$.

$$\begin{array}{ccc} K & \xrightarrow{\varphi} & K' \\ \downarrow & & \downarrow \\ K(\alpha) & \xrightarrow{\psi} & K'(\alpha') \\ \downarrow & & \downarrow \\ \Sigma & \xrightarrow{\alpha} & \Sigma' \end{array}$$

On peut prolonger $\varphi$ en un isomorphisme $\psi : K(\alpha) \to K'(\alpha')$ tel que $\psi(\alpha) = \alpha'$

$\begin{cases} \Sigma = \text{corps des racines de } f \text{ sur } K(\alpha) \\ \Sigma' = \quad " \quad " \quad \text{de } f' \text{ sur } K'(\alpha') \end{cases}$

et $[\Sigma ; K(\alpha)] = \frac{n}{d} < n$.

On applique l'hypothèse de récurrence : on peut prolonger $\varphi$ par $\alpha$ : $\Sigma \to \Sigma'$. CQFD

---

Co | Deux corps des racines $\Sigma$ et $\Sigma'$ de $f \in K[X]$ sont isomorphes.
On peut trouver $\varphi : \Sigma \xrightarrow{\sim} \Sigma'$ tel que les éléments de $K$ soient invariants.

---

Il suffit d'appliquer le th. précédent avec :

$K' = K$ et $\varphi = Id_K$

On a le diagramme :

$$\begin{array}{ccc} K & \xrightarrow[\sim]{Id} & K \\ \downarrow & & \downarrow \\ \Sigma & \xrightarrow[\sim]{\varphi} & \Sigma' \end{array} \quad \text{et } \varphi|_K = Id_K$$

## 2°/ Application

Th | Soit $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$.
Il existe un unique corps à $p^n$ éléments, noté $\mathbb{F}_{p^n}$ (à isomorphisme près)

Rappelons qu'un corps $K$ de caractéristique $p \in \mathcal{P}$ est forcé

mment de cardinal $p^n$ :

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow K \qquad \text{car } K = p \qquad \# K = p^n$$

Les éléments de K sont des racines de $X^{p^n} - X \in \mathbb{F}_p[X]$ puisque $\# K^* = K \setminus \{0\}$ est de cardinal $p^n - 1$, et que

$$\forall x \in K^* \quad x^{p^n - 1} = 1$$

$\# K = p^n$ et K est un corps de décomposition de $X^{p^n} - X$ puisque $X^{p^n} - X$ possède au plus $p^n$ racines. K est un corps des racines car il possède exactement $p^n$ ~~ra~~ éléments.

CQFD.

<u>Remarque</u> :

Soit $L \supset \mathbb{F}_p$ un corps dans lequel $X^{p^n} - X$ possède toutes ses racines. Alors l'ensemble de ces racines forme un corps $\Omega$ puisque
$$\begin{cases} (x_1 x_2)^{p^n} = x_1 x_2 \\ (x_1 + x_2)^{p^n} = x_1^{p^n} + x_2^{p^n} \text{ dans } \mathbb{F}_p \end{cases}$$
et, de plus, $\Omega \simeq \mathbb{F}_{p^n}$ puisque toutes les racines de $X^{p^n} - X$ sont distinctes (cf. $(X^{p^n} - X)' = \underbrace{p^n}_{0} X^{p^n - 1} - 1 = -1$ (caractéristique $(\mathbb{F}_p) = p$)

Pro | Soit $\mathbb{F}_q$ $(q = p^n)$ un corps fini et $n \geq 2$. Il existe au moins un polynôme $P \in \mathbb{F}_q[X]$ irréductible sur $\mathbb{F}_q[X]$ et de degré $n$.

Preuve : voir TD n° 8.

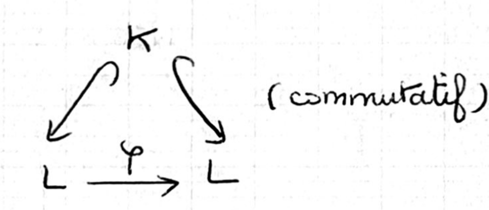
Moralement, plus le corps est de cardinal élevé et moins il y a de polynômes irréductibles sur ce corps.

Théorie de Galois

## 1°/ Groupe de Galois : Définition

Def | Soient $P \in K[X]$ et $L$ le corps des racines de $P$.
On appelle "groupe de galois du polynôme $P \in K[X]$" le groupe des automorphismes du corps $L$ laissant fixe $K$ :

$$\boxed{Gal_K(P) = Aut_K(L)}$$




Nous allons considérer un exemple, puis passer à la théorie :

## 2°/ Exemple

Considérons le polynôme $X^4 - 3 \in \mathbb{Q}[X]$. Il est irréductible sur $\mathbb{Q}[X]$ d'après le critère d'Einseinstein. Posons $r = \sqrt[4]{3} \in \mathbb{C}$

$$X^4 - 3 = (X - r)(X + r)(X - ir)(X + ir)$$

Le corps des racines de $P(X) = X^4 - 3$ est $L = \mathbb{Q}(i, r)$.

$[L ; \mathbb{Q}] = 8$ et une $\mathbb{Q}$-base de $L$ est

$$(1, r, r^2, r^3, i, ir, ir^2, ir^3)$$

Remarque 1 :

Tout automorphisme $\varphi \in Aut_K(L)$ permute les racines de $X^4 - 3$.

En effet :

$\xi$ racine de $X^4 - 3$

Alors $\quad \xi^4 - 3 = 0 \Rightarrow \varphi(\xi^4 - 3) = 0$

$\Rightarrow \varphi(\xi)^4 - \varphi(3) = 0 \Rightarrow \varphi(\xi)^4 - 3 = 0$

+ <u>Remarque 2</u> : $\varphi \in Aut_K(L)$ est parfaitement déterminé par la donnée de $\varphi(r)$ et de $\varphi(i)$.
C'est évident puisque $L = \mathbb{Q}(r, i)$.

Ici : $\varphi(r) \in \{r, -r, ir, -ir\}$
de m̂ : $\varphi(i) \in \{i, -i\}$ (considérer $i^2+1=0$)
et réciproquement, n'importe quel choix convient, et définit $\varphi$.
Ainsi :

$$\# Aut_K(L) = 8$$

Notons :

$S : \begin{cases} S(r) = ir \\ S(i) = i \end{cases}$ $T : \begin{cases} T(r) = r \\ T(i) = -i \end{cases}$ (restriction de la conjugaison)

Quels sont les ordres de ces éléments de $Aut_K(L)$ ?
$S^2(r) = S(i) S(r) = -r$
$S^3(r) = -ir$
$S^4(r) = r$
Mais $S^4(i) = i$ $\Big\} \Rightarrow S^4 = Id$ et $\omega(S) = 4$

T est d'ordre 2. En effet :

$$T^2(i) = i \quad \text{et } T^2(r) = r \quad \Rightarrow T^2 = Id_L$$

Parmi les groupes commutatifs à 8 éléments, il y a 3 possibilités :

$$(\mathbb{Z}/2\mathbb{Z})^3 \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \qquad \text{ou} \qquad \mathbb{Z}/8\mathbb{Z}$$

$Aut_K(L)$ possède un élément d'ordre 4 et un élément d'ordre 2, et il se peut que ce soit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/8\mathbb{Z}$

Notons $\mathcal{I}s$(carré) le groupe des isométries du carré. On peut montrer que l'application

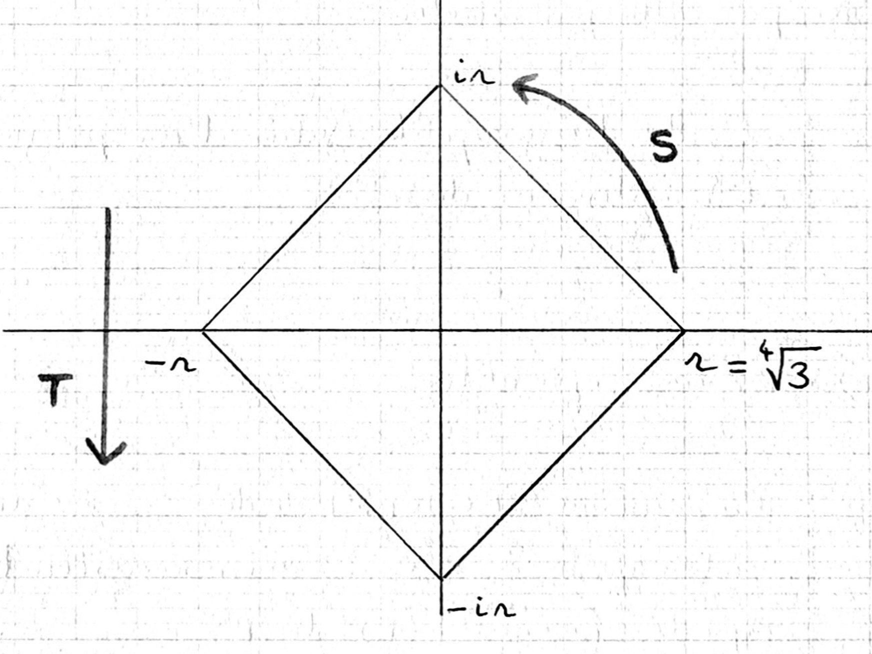
$$\Psi : \mathrm{Aut}_k(L) \longrightarrow \mathcal{I}s(\text{carré})$$
$$S\,;\,T \longmapsto r_{0,\frac{\pi}{2}}\,,\, s_{Ox}$$

est un isomorphisme de groupes. groupe diédral $\Delta_4$

$G = \{1, S, S^2, S^3, T, ST, S^2T, S^3T\}$

sous-groupe distingué cyclique d'ordre 4 (car $S^3T = T\circ S$ d'où $TST = S^3 = S^{-1}$ et $\{1, S, S^2, S^3\}$ invariant par tout automorphisme intérieur)

<u>Remarque</u> : <u>Interprétation géométrique</u>.




3°/ <u>Théorie de Galois</u>.

Def | On note parfois $K(P) = L$ le corps des racines du polynôme $P \in K[X]$

On rappelle que :

**Def** Le groupe de Galois du polynôme $P \in K[X]$ le groupe des automorphismes du corps $K(P)$ laissant fixe $K$ :

$$\text{Gal}_K(P) = \text{Aut}_K(K(P))$$

**Th** Le groupe de Galois $\text{Gal}_K(P)$ est isomorphe à un groupe de permutation des racines $\{\alpha_1, \dots, \alpha_n\}$ de $P$.

(racines distincts $\alpha_1, \dots, \alpha_k$ de $P$)

En effet, si $S \in \text{Gal}_K(P)$, alors $S|_{\{\alpha_1, \dots, \alpha_n\}}$ détermine une permutation de $\{\alpha_1, \dots, \alpha_n\}$, et $S$ est complètement déterminée par cette permutation.

**Co** L'ordre du groupe de Galois d'un polynôme de degré $n$ est un diviseur de $n!$

a) Extensions séparables.

**Def** Un polynôme $P \in K[X]$ de degré $n$ est dit "séparable" sur le corps $K$ s'il a $n$ racines distinctes dans le corps des racines $K(P)$ de $P$.

Sinon, $P$ est dit "inséparable".

Une extension finie $M \supset K$ est dite séparable sur $K$ si tout élément de $M$ est racine d'un polynôme séparable sur $K$.

Pro | P est séparable ssi $\Delta(P, P') = 1$

Preuve :

$P = c(X-u_1)^{e_1} \cdots (X-u_k)^{e_k}$

$u_1, \dots, u_k \in L = K(P)$

La dérivée formelle de P est :

$P' = ce_1(X-u_1)^{e_1-1}(X-u_2)^{e_2} \cdots (X-u_k)^{e_k} + \dots + ce_k(X-u_1)^{e_1} \cdots (X-u_k)^{e_k-1}$

On remarque que :

$$\begin{cases} (X-u_1) \mid P' \text{ ssi } e_1 > 1 \\ \text{-------} \\ (X-u_k) \mid P' \text{ ssi } e_k > 1 \end{cases}$$

Ainsi :

$e_1 = \dots = e_k = 1 \iff (X-u_i)$ ne divise pas $P'$

$(i \in [1, k])$

Tous les diviseurs premiers de P sont les $X-u_i$, d'où :

$e_1 = \dots = e_k = 1 \iff \Delta(P, P') = 1$

Co | Un polynôme irréductible est séparable à moins que sa dérivée formelle ne soit nulle.

En effet : $P \in K[X]$ irréductible

$\Delta(P, P') = 1 \iff P \nmid P' \iff P' \neq 0$ (car $\deg P' < \deg P$)

Co | Tout polynôme irréductible sur un corps de caractéristique $\infty$ est séparable.

En effet : $f' = na_n X^{n-1} + \dots \neq 0$ si $n > 0$ et $a_n \neq 0$.

b) Théorèmes de base.

Z

**Th 1** | Soit $P \in K[X]$ un polynôme séparable, $K(P)$ désigne le corps des racines de $P$ :

$$\#(gal_K(P)) = [K(P) ; K]$$

Z

**Th 2** | Dans le corps des racines $K(P)$ d'un polynôme séparable, les éléments qui restent invariants dans tout automorphisme du groupe de galois $Aut_K(K(P))$ sont ceux de $K$ et seulement ceux là. On notera :

$$K = K(P)^{gal_K(P)}$$

(NB : par définition, si $G$ opère sur $X$, on note

$$X^G = \{x \in X \ / \ \forall g \in G \quad gx = x\}$$

Preuve 1 :

Il faut compléter la démonstration de l'unicité du corps des racines $L = K(P)$ de la façon suivante :

**Lemme** | $P \in K[X]$ séparable. Un isomorphisme $\varphi$ de $K$ sur $K'$ se prolonge en un isomorphisme $\alpha$ de $L$ sur $L'$ laissant $K$ fixe, et il existe exactement $[L : K]$ choix possibles pour $\alpha$.

$$\begin{array}{ccc} K & \xrightarrow{\varphi} & K' \\ \downarrow & & \downarrow \\ L & \xrightarrow{\alpha} & L' = K'(P') \end{array} \qquad P' = \varphi(P)$$

La 1<sup></sup>re partie du lemme a déjà été montrée.

La seconde partie se montre par récurrence sur $n = [L ; K]$

- Vrai pour $n=1$
- Vrai au rang $n$

Soit $x \in L \setminus K \ / \ P(x) = 0$ et $Q$ le polynôme minimal de $x$

$$\begin{array}{ccc} K & \xrightarrow{\varphi} & K' \\ \downarrow & & \downarrow \\ K(x) = K_1 & \xrightarrow{\alpha_1} & K_1' = K'(x') \\ \downarrow & & \downarrow \\ L & \xrightarrow{\alpha} & L' \end{array}$$

(1)

$x'$ est une racine de $\varphi(Q) = Q'$. (2).

Posons $\deg Q = d$. Comme $P$ est séparable, son diviseur $Q'$ de degré $d$ aura exactement $d$ racines distinctes $x'$. Ces $d$ choix donnent exactement $d$ choix pour $\alpha_1$ dans (1).

$L$ = corps des racines de $P$ dans $K_1$. L'hypothèse récurrente nous donne $\frac{n}{d} = [L ; K_1]$ choix possibles pour prolonger $\alpha_1$ en $\alpha : L \to L'$.

En tout, il y aura $d \cdot \frac{n}{d} = n$ prolongements possibles,

CQFD.

On applique ce lemme avec $\varphi = Id_K$. On trouve :

$$\# gal_K(P) = [K(P) ; K].$$

<u>Preuve 2</u> :

Soit $M \doteq K(P)^{gal_K(P)}$

* $K \subset M$
* $M$ est un corps

$x, y \in K(P)^{gal_K(P)}$ $\forall g \in gal_K(P)$ $g(x-y) = g(x) - g(y) = x - y$

$x \in K(P)^{gal_K(P)}$ $y \in K(P)^{gal_K(P)*}$ $\forall g \in gal_K(P)$ $g(xy^{-1}) = g(x)\, g(y)^{-1}$

* On a le diagramme :

$$\begin{array}{ccc} K & \xrightarrow{Id} & K \\ \downarrow & & \downarrow \\ M & \xrightarrow{Id} & M \\ \downarrow & & \downarrow \\ K(P) & \xrightarrow[g]{} & K(P) \end{array}$$

Comme $M = K(P)^{gal_K(P)}$ on a : $gal_K(P) = gal_M(P)$

(penser à $Aut_K(K(P)) = Aut_M(K(P))$ )

Mais alors :

$$\underbrace{[K(P) ; K]}_{\# gal_K(P)} = \underbrace{[K(P) ; M]}_{\# gal_M(P)} [M ; K] \quad \text{(cf Th 1) car } P \text{ est séparable}$$

d'où $[M ; K] = 1 \Leftrightarrow M = K$ CQFD

c)

Soit $P \in K[X]$ , et $L = K(P)$ le corps des racines.

$\mathcal{K}$ = ensemble des sous-extensions de $L$ pour $K = \{M / K \subset M \subset L\}$

$\mathcal{G} = \{$ sous-groupes $H$ de $G = gal_K(P)\}$

$\mathcal{K}$ $\qquad\qquad$ $\mathcal{G}$

$K \subset M \subset L$ (corps) $\longrightarrow$ $H \subset G = gal_K(P)$

On définit :

$$\mathcal{K} \underset{h}{\overset{k}{\rightleftarrows}} \mathcal{G}$$

par :

$M \in \mathcal{K}$ $\quad h(M) = \{g \in \mathcal{G} \ / \ \forall m \in M \quad g(m) = m\} = gal_M(P)$

$H \subset G$ $\quad k(H) = L^H = \{x \in L \ / \ \forall g \in H \quad g(x) = x\}$

**Th** | Soit $P \in K[X]$ un polynôme séparable. Avec les notations signalées :

$$\begin{cases} h \circ k = Id_{\mathcal{G}} \\ k \circ h = Id_{\mathcal{K}} \end{cases}$$

c.à.d $h$ et $k$ sont bijectives.

Preuve :

a) <u>$h$ injective</u>

$M_1$ et $M_2$ sont 2 corps tels que $h(M_1) = h(M_2)$

$$h(M_1) = gal_{M_1}(P) = gal_{M_2}(P) = h(M_2)$$

d'où :

$$\begin{cases} M_1 = K(P)^{gal_{M_1}(P)} \\ M_2 = K(P)^{gal_{M_2}(P)} \end{cases} \Rightarrow M_1 = M_2 \qquad \text{(cf. Th 2)}$$

b) <u>$h \circ k = Id_{\mathcal{G}}$</u>

$$H \mapsto k(H) \mapsto h \circ k(H) = gal_{k(H)}(P)$$

donc $H \subset h \circ k(H)$

**lemme** : Soit $L$ ; $H \subset Aut(L)$ et $M = L^H \subset L$
On a $[L : L^H] \leq \# H$ (Emil Artin)

En effet, si $H = \{S_1, \dots, S_n\}$, soient $c_1, \dots, c_{n+1} \in L$.
Montrons que ces $n+1$ éléments forment un système $L^H$-lié.
On cherche donc $(x_1, \dots, x_{n+1}) \in M^{n+1}$ non tous nuls et tels que

$$x_1 c_1 + \dots + x_{n+1} c_{n+1} = 0$$

Alors :

$$\begin{cases} x_1 S_1(c_1) + \dots + x_{n+1} S_1(c_{n+1}) = 0 \\ \dots\dots\dots \\ x_1 S_n(c_1) + \dots + x_{n+1} S_n(c_{n+1}) = 0 \end{cases} \qquad (1)$$

Désignons par $r$ le rang de la matrice $(S_i(c_j))_{\substack{1\le i\le n \\ 1\le j\le n+1}}$ et supposons que

$$\overset{1 \dots r}{\left( S_i(c_j) \right)} \begin{matrix} 1 \\ \vdots \\ r \end{matrix} \quad \text{de rang } r.$$

$$\underbrace{\begin{pmatrix} S_1(c_1) & \dots & S_1(c_{r+1}) \\ \vdots & \ddots & \\ S_r(c_1) & \dots & S_r(c_{r+1}) \end{pmatrix}}_{rg\, r} \begin{pmatrix} x_1 \\ \vdots \\ x_{r+1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \qquad (2)$$

admet une droite vectorielle comme solution, puisque $\dim \operatorname{Ker} f = (r+1) - r$.

Quitte à changer l'ordre des variables, on peut trouver une solution de la forme

$$(1, x_2, \dots, x_{r+1})$$

En observant (1), on constate que :

$$x_1 S_1(c_1) + \dots + x_{n+1} S_1(c_{n+1}) = 0 \qquad (x_i \in L^H;\ c_i \in L;\ S_i \in H)$$

$$S(x_1)\ S\circ S_1(c_1) + \dots + S(x_{n+1})\ S\circ S_1(c_{n+1}) = 0 \qquad \forall S \in H$$

$\forall S \in H \qquad (S(1), S(x_2), \dots, S(x_{r+1}))$ solution de (2)

$S(1) = 1$ ($S$ automorphisme de corps)

d'où :

$$\begin{cases} S(x_2) = x_2 \\ \vdots \\ S(x_{r+1}) = x_{r+1} \end{cases} \Rightarrow \exists\, x_1, \dots, x_{r+1} \in M^{r+1} \text{ vérifiant :}$$

$$\underset{\substack{\not\,\\ 0}}{x_1} c_1 + \dots + x_{r+1} c_{r+1} + \dots + \underbrace{x_{n+1} c_{n+1}}_{0} = 0$$

d'où $[L ; L^H] \leq \# H$.

Retour au b)

On avait

$H \subset hk(H)$

$\# hk(H) = [L, L^H] \leq \# H$ d'après le lemme d'Artin.

car $hk(H) = \text{gal}_{k(H)}(P)$

Donc $hk(H) = H$.

CQFD

Théorème de Wedderburn | Tout corps fini est commutatif

1°/ Préliminaires.

K corps. Le centre $Z(K)$ est l'ensemble des éléments qui commutent avec tous les éléments de K.

$Z(K) = \{ z \in K \ / \ \forall a \in K \quad az = za \}$ = sous-corps de K

Soit $a \in K$ fixé, alors $N_a = \{ x \in K \ / \ xa = ax \}$ est un sous-corps de K. Manifestement : $Z(K) = \bigcap_{a \in K} N_a$ et $Z(K) \subset N_a \subset K$.

Si K est fini :

$car(K) = \text{Inf} \{ n > 0 \ / \ n.1 = 0 \} < \infty$

Alors : $\{ \underline{0}, \underline{1}, 2, \dots, n.1, \dots \} \simeq \mathbb{Z}/p\mathbb{Z} \hookrightarrow K$. C'est le plus petit corps inclus dans K ("sous-corps premier de K").

On a : $\mathbb{Z}/p\mathbb{Z} \hookrightarrow Z(K) \subset N_a \subset K$ (1)

Ainsi : $\begin{cases} \# Z(K) = q = p^\alpha \\ \# N_a = q^{n_a} \\ \# K = q^N \end{cases}$

Des inclusions (1), on tire aussi la suite :

$$Z(K)^* \subset N_a^* \subset K^*$$

d'où $q-1 \mid q^{n_a}-1 \mid q^N - 1$

Action de $K^*$ sur $K^*$ par conjugaison :

$$K^* \times K^* \longrightarrow K^*$$
$$(x, y) \longmapsto xyx^{-1}$$

La formule des classes donne :

$$\# K^* = \sum \#(\text{orbites})$$

$G.y \simeq G/N_y$ $\quad N_y$ = stabilisateur de y.

Ici : $\{x y x^{-1} / x \in K^*\} \simeq K^* / N_y^*$

La formule des classes donne :

$$\# K^* = \sum \# (\text{classes de conjugaison})$$

$$q^N - 1 = \underbrace{q-1}_{\# Z(K^*)} + \sum_{\substack{n_y \neq N \\ n_y \mid N}} \underbrace{\frac{q^N - 1}{q^{n_y} - 1}}_{\# (K^* / N_y^*)} \qquad (0)$$

L'astuce du théorème de Wedderburn consiste à montrer qu'une telle décomposition est impossible si K non commutatif, c.à.d si la $\sum$ somme est non vide.

## 2°/ Polynômes cyclotomiques.

$X^N - 1 \in \mathbb{Q}[X]$

Les racines de $X^N - 1$ dans $\mathbb{C}$ sont $\{e^{i \frac{2\pi}{N} k} / k = 0, \dots, N-1\} = U_N$

$U_N$ forme un groupe multiplicatif isomorphe à $\mathbb{Z}/N\mathbb{Z}$.

Les racines primitives N-ièmes de l'unité sont, par définition les éléments de $U_N$ qui sont d'ordre N. Il y en a $\varphi(N)$

Dans $\mathbb{C}[X]$ :

$$X^N - 1 = \prod_k (X - e^{i \frac{2\pi}{N} k}) = \prod_{\delta(k,N)=1} (X - e^{i \frac{2\pi}{N} k}) \cdot \prod_{\delta(k,N) \neq 1} (X - e^{i \frac{2\pi}{N} k})$$

On pose :

<u>Def</u> : $F_N(X) = \prod_{\substack{\delta(k,N)=1 \\ k=0,\dots,N-1}} (X - e^{i \frac{2\pi}{N} k})$ est appelé le polynôme

cyclotomique d'ordre $N$.

Th | $F_n(X) \in \mathbb{Z}[X]$

On a : $X^N - 1 = \prod_{n|N} F_n(X)$

$F_1(X) = X - 1$
$F_2(X) = X + 1$
$F_3(X) = X^2 + X + 1$
$F_4(X) = X^2 + 1$

Preuve : récurrence sur $N$ $\quad F_N(X) = \dfrac{X^N - 1}{\prod_{\substack{n|N \\ n<N}} F_n(X)} \in \mathbb{C}[X]$

$F_n(X)$ est monique (produit de polynômes moniques) et $X^N - 1 \in \mathbb{Z}[X]$
donc $F_N(X) \in \mathbb{Z}[X]$. (lemme laissé au lecteur)

## 3°/ Démonstration du théorème de Wedderburn

$$\frac{q^N - 1}{q^{n_y} - 1} = \frac{\prod_{n|N} F_n(q)}{\prod_{n|n_y} F_n(q)} = \prod_{\substack{n|N \\ n \nmid n_y}} F_n(q) = \text{multiple de } F_N(q)$$

(car $F_N(q)$ est au numér. sans être au dénom.)

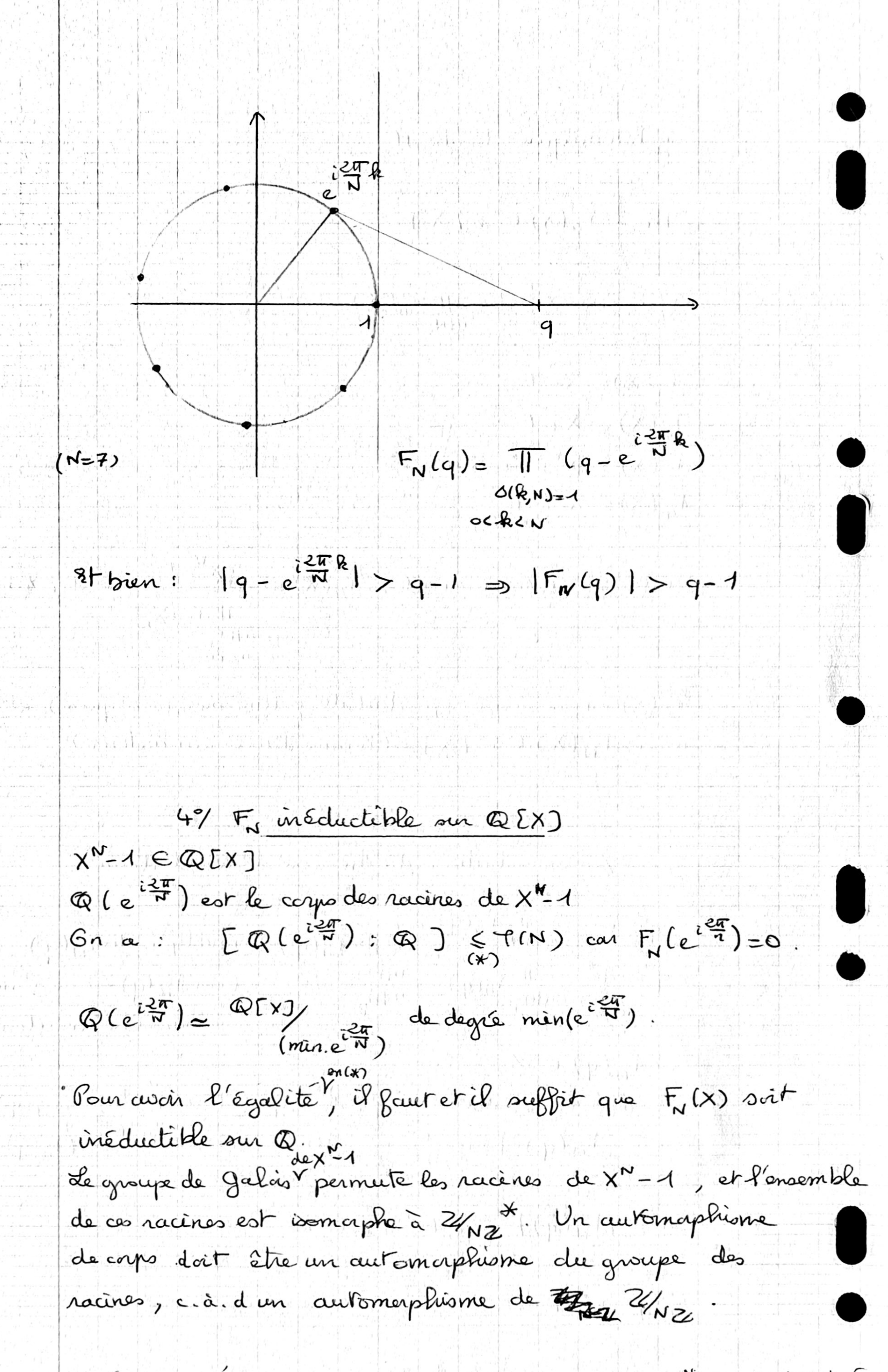
et $F_N(q) \in \mathbb{Z}$

La formule (0) donne : $q^N - 1 = q - 1 + \sum \dfrac{q^N - 1}{q^{n_y} - 1}$ et $\begin{cases} F_N(q) \mid q^N - 1 \\ F_n(q) \mid \dfrac{q^N - 1}{q^{n_y} - 1} \end{cases}$

Donc $F_N(q) \mid q - 1$ (1)

or $|F_N(q)| > q - 1$ (2)

(2) provient de :




$$F_N(q) = \prod_{\substack{\delta(k,N)=1 \\ 0<k<N}} \left(q - e^{i\frac{2\pi}{N}k}\right)$$

Et bien : $\left|q - e^{i\frac{2\pi}{N}k}\right| > q-1 \Rightarrow |F_N(q)| > q-1$

## 4°/ $F_N$ irréductible sur $\mathbb{Q}[X]$

$X^N - 1 \in \mathbb{Q}[X]$

$\mathbb{Q}(e^{i\frac{2\pi}{N}})$ est le corps des racines de $X^N-1$

On a : $[\mathbb{Q}(e^{i\frac{2\pi}{N}}) : \mathbb{Q}] \underset{(*)}{\leq} \varphi(N)$ car $F_N(e^{i\frac{2\pi}{N}}) = 0$.

$\mathbb{Q}(e^{i\frac{2\pi}{N}}) \simeq \mathbb{Q}[X] / (\min . e^{i\frac{2\pi}{N}})$ de degré $\min(e^{i\frac{2\pi}{N}})$.

· Pour avoir l'égalité en (*), il faut et il suffit que $F_N(X)$ soit irréductible sur $\mathbb{Q}$.

Le groupe de Galois de $X^N-1$ permute les racines de $X^N-1$, et l'ensemble de ces racines est isomorphe à $\mathbb{Z}/N\mathbb{Z}^*$. Un automorphisme de corps doit être un automorphisme du groupe des racines, c.à.d un automorphisme de ~~$\mathbb{Z}$~~ $\mathbb{Z}/N\mathbb{Z}$.

(* Cas intéressant ici : l'ensemble des racines de $X^N-1$ est structuré en groupe mult. isomorphe à $\mathbb{Z}/N\mathbb{Z}$. $G \longrightarrow \mathfrak{S}_n$, $s \longmapsto s|_{\{a_1,\dots,a_n\}} \in Aut(\{a_1,\dots,a_n\}) \simeq Aut(\mathbb{Z}/n\mathbb{Z})$ )

Mais $\text{Aut}\,\mathbb{Z}/_{N\mathbb{Z}} \simeq \mathcal{U}(\mathbb{Z}/_{N\mathbb{Z}}) \Rightarrow \#\,\text{Aut}(\mathbb{Z}/_{N\mathbb{Z}}) = \varphi(N)$
d'où :
$\#\,\text{gal}_{\mathbb{Q}}(X^n-1) = [\,\mathbb{Q}(e^{i\frac{2\pi}{n}}) : \mathbb{Q}\,] = \varphi(N)$

Ainsi $[\,\mathbb{Q}(e^{i\frac{2\pi}{N}}) ; \mathbb{Q}\,] = \varphi(N)$. $\Rightarrow$ $F_N$ irréductible sur $\mathbb{Q}[X]$
On a démontré le théorème ci-dessous,

Th | $F_N(X)$ est irréductible sur $\mathbb{Q}[X]$.